W. M. MILLER, Marquette University
E. C. MOLINA, American Tel. and Tel. Co., New York
C. N. MOORE, University of Cincinnati
T. W. MOORE, Indiana University
W. L. MOORE, University of Louisville
C. C. MORRIS, Ohio State University
MAX MORRIS, Case School of Applied Science
PAUL MUEHLMAN, St. Louis University
F. D. MURNAGHAN, Johns Hopkins University
J. R. MUSSELMAN, Western Reserve University

J. H. NEELLEY, Carnegie Institute of Technology
J. P. NICKOL, St. Bonaventure's College
J. A. NYSWANDER, University of Michigan

RUFUS OLDENBURGER, University of Michigan
E. G. OLDS, Carnegie Institute of Technology
H. L. OLSON, Michigan State College
OYSTEIN ORE, Yale University
F. W. OWENS, Pennsylvania State College

L. J. PARADISO, Cornell University
R. S. PARK, Eastern Teachers College, Richmond, Ky.
B. C. PATTERSON, Hamilton College
T. S. PETERSON, University of Michigan
L. C. PLANT, Michigan State College
T. M. PUTNAM, University of California

G. Y. RAINICH, University of Michigan
S. E. RASOR, Ohio State University
S. W. REAVES, University of Oklahoma
MINA S. REES, Hunter College
W. T. REID, National Research Fellow, University of Chicago
C. N. REYNOLDS, Jr., West Virginia University
C. E. RHODES, University of Cincinnati
R. G. D. RICHARDSON, Brown University
P. R. RIDER, Washington University
H. L. RIETZ, University of Iowa
C. F. ROOS, Cornell University
S. A. ROWLAND, Ohio Wesleyan University
LULU L. RUNGE, University of Nebraska

S. T. SANDERS, Louisiana State University
GEORGE SAUTÉ, Cleveland College
MAURICE SCHEIER, St. Bonaventure's College
HAZEL E. SCHOONMAKER, New Jersey College for Women
G. T. SELLEW, Knox College
H. C. SHAUB, Washington and Jefferson College
W. F. SHENTON, American University
L. S. SHIVELY, Ball State Teachers College, Munice, Ind.
C. A. SHOOK, Yale University
C. GRACE SHOVER, Connecticut College
W. G. SIMON, Western Reserve University
LAO G. SIMONS, Hunter College
H. E. SLAUGHT, University of Chicago
L. L. SMAIL, Lehigh University
SISTER M. PAULINE SMYTH, Aquinas Institute
A. E. STANILAND, University of Pittsburgh
H. E. STELSON, Kent State College
EUGENE STEPHENS, Washington University
GUY STEVENSON, University of Louisville
K. D. SWARTZEL, University of Pittsburgh
J. L. SYNGE, University of Toronto

J. D. TAMARKIN, Brown University
J. H. TAYLOR, George Washington University
J. S. TAYLOR, University of Pittsburgh
C. F. THOMAS, Case School of Applied Science
M. O. TRIPP, Wittenberg College
BIRD M. TURNER, West Virginia University

J. H. WEAVER, Ohio State University
F. M. WEIDA, George Washington University
MARIE J. WEISS, Sophie Newcomb College
E. D. WELLS, University of Pittsburgh
WILLIS WHITED, Pennsylvania State Highway Dept.
E. A. WHITMAN, Carnegie Institute of Technology
G. T. WHYBURN, John Hopkins University
R. L. WILDER, University of Michigan
K. P. WILLIAMS, Indiana University
C. O. WILLIAMSON, College of Wooster
F. L. WREN, George Peabody College

B. F. YANNEY, College of Wooster
C. H. YEATON, Oberlin College
J. W. Young, Dartmouth College

B. C. ZIMMERMAN, Marquette University

The sessions of the American Association for the Advancement of Science began on Monday evening with an address in the Music Hall of the Cleveland Public Auditorium by the retiring president, Doctor Robert A. Millikan, on

"Atomic disintegration and atomic synthesis." Following this the scientists were received in the ballroom of the Public Auditorium by the general officers of the American Association with President and Mrs. R. E. Vinson of Western Reserve University and President and Mrs. W. E. Wickenden of Case School of Applied Science. Among other general sessions of the American Association were the Sigma Xi lecture on "The science of photography" by Doctor C. E. K. Mees of the Eastman Kodak Company on Tuesday evening; an illustrated lecture on "Searching out Pluto, Lowell's trans-Neptunian planet" by R. L. Putnam, trustee of the Lowell Observatory, and Doctor V. M. Slipher, director of the Lowell Observatory, on Wednesday evening; and an illustrated lecture on "Weighing the earth" by Doctor P. R. Heyl of the U. S. Bureau of Standards on Friday evening. On Tuesday afternoon the eighth Josiah Willard Gibbs lecture was given by Doctor E. B. Wilson of the Harvard School of Public Health. This address was given under the joint auspices of the American Association and the American Mathematical Society. A large audience listened with great interest as Professor Wilson spoke on "Reminiscences of Gibbs by a student and colleague."

The annual science exhibition was housed in the gymnasium of Western Reserve University in which also the general registration offices were located. The Cleveland exhibition was larger and more varied than usual and consisted of exhibits of scientific apparatus by numerous institutions and firms as well as exhibits by a considerable number of book publishers. Of special interest to mathematicians were Doctor P. R. Heyl's models of the regular four-dimensional solids.

The science meetings were for the most part held on and about the grounds of Case School of Applied Science and Western Reserve University, although some of the societies in the social sciences held their meetings in the Cleveland hotels. This concentration of meetings in the University district enabled the scientists to go readily from one program to another when this was desired. The general local arrangements for the Cleveland meetings were in charge of Doctor H. W. Mountcastle; he and his associates were very effective in organizing the plans for the Cleveland meetings and many expressions of appreciation of their work were heard.

Professor Dunham Jackson and Secretary Cairns represented the Mathematical Association on the Council of the American Association, which met Monday afternoon and each morning thereafter for the transaction of general business. Doctor C. F. Roos, assistant professor of mathematics at Cornell University, was elected Permanent Secretary of the American Association in succession to Doctor Burton E. Livingston, who has held that office since 1920; Doctor Livingston will continue as an officer of the American Association in the capacity of General Secretary. Professor E. R. Hedrick was elected vice-president and chairman of Section A for the year 1931.

The Hotel Statler was the headquarters for the mathematicians, and convenient facilities were put at their disposal for committee rooms, for small

dinners, and for the joint dinner of the mathematicians which was held Wednesday evening. At this last dinner brief speeches were made by the presiding officer, President E. R. Hedrick, and by Professors E. T. Bell, L. P. Eisenhart, and President J. W. Young. At the close of this dinner a resolution, presented by Professor Carmichael, was adopted expressing the gratitude of the mathematicians for the kindness and generosity shown by our hosts and for the effective planning which made the meetings pleasant and successful.

The American Mathematical Society held a joint session on Monday afternoon with Section K of the American Association and the American Statistical Association at which there were papers by Professor G. C. Evans on "Simple types of economic crises and cycles," by Professor Ragnar Frisch on "A method of decomposing an empirical series into its cyclical and progressive components," and by Professor Harold Hotelling on "Recent improvements in statistical inference." The Society held sessions on Tuesday and Wednesday mornings in three sections for the reading of papers. The Society's Gibbs lecture has already been mentioned.

The program of the Mathematical Association consisted of a joint session with Section A and the Society on Wednesday afternoon and two sessions on Thursday. The excellent program was prepared by a committee consisting of Professors C. C. MacDuffee, F. W. Owens, A. H. Wilson, and W. G. Simon, Chairman. President Young presided at the morning session and Professor Carmichael at the afternoon session, being replaced by Vice-President C. N. Moore for the last part of the program. The program follows, together with abstracts of some of the papers, numbered in accordance with their place on the program.

Joint Session of the Association with the Society and Section A of the American Association

1. "Mathematics and speculation" by Professor E. T. Bell, California Institute of Technology, retiring vice-president of Section A of the American Association.

2. "Recent developments in abstract algebra" by Professor Oystein Ore, Yale University, by invitation of the Association and the Society.

3. "Axiomatical theory of dimension" by Professor Karl Menger, University of Vienna, at the request of the Mathematical Society.

1. The address by Professor Bell was published in the March, 1931 issue of the *Scientific Monthly*.

First Session of the Association

1. "Early history of the American Mathematical Monthly" by Professor B. F. Finkel, Drury College.

2. "Analysis situs as a branch of elementary geometry" by Professor J. W. Alexander, Princeton University.

3. "The equilateral hyperbola" by Professor J. R. Musselman, Western Reserve University.

1. It was the good fortune of the Mathematical Association to have Professor Benjamin F. Finkel, founder and first editor of the MATHEMATICAL MONTHLY, present a full record of its early history. Many questions have been frequently raised as to the establishment and development of the MONTHLY in the years before it became the official organ of the Mathematical Association. This authoritative record will appear in the MONTHLY later in the year.

2. It is hoped that the excellent expository paper by Professor Alexander will appear in the MONTHLY at an early date.

3. From the standpoint of analytical geometry the ellipse and hyperbola are treated without partiality in all textbooks. Yet when the special case of each is discussed we find a whole chapter devoted to the circle, while usually one paragraph suffices for the equilateral hyperbola. Why should this be? The ease with which a circle can be constructed can only account partly for it; the blame must be put upon Plato and his followers. Plato, who had such an extraordinary influence upon the geometers of his time, insisted upon permitting in construction problems those instruments only which amount, analytically, to the straight line and the specialized ellipse. It is due to him that our geometry today is one-sided.

Professor Musselman then showed that Menaechmus about the middle of the fourth century B.C., used the equilateral hyperbola in one solution of the problem of duplicating the cube. The problem of trisecting any angle can be reduced to finding the intersection of a circle and an equilateral hyperbola. The mechanical device for constructing an equilateral hyperbola, due to H. H. S. Cunynghame,* when the asymptotes or the axes are known, would be useful for this purpose.

The study of the curve analytically can be simply done by using the Cartesian form $xy=c^2$ and expressing the coordinate of a point on the curve parametrically as $x=ct$, $y=c/t$. A number of interesting theorems concerning sets of points on the curve were used to illustrate the possibilities of this curve as a subject for further study in our elementary courses. Since the strophoid and lemniscate are inverses of the equilateral hyperbola, a knowledge of the latter is helpful in studying the former curves. But the equilateral hyperbola is worth studying for its own sake.

SECOND SESSION OF THE ASSOCIATION

1. "Mathematics in Hungary" by Professor TIBOR RADÓ, Ohio State University.

2. "Remainder terms in interpolation formulas" by Professor J. F. REILLY, University of Iowa.

3. "Theoretical and statistical investigations concerning the interrelations of demand, cost of production and profit" by Professor C. F. ROOS, Cornell University.

---

* Taylor, Ancient and Modern Geometry of Conics, p. 177.

1. In order to depict the character of preparatory mathematics in the secondary and early collegiate courses in Hungary, Professor Radó described the competitive examinations for the Eötvös Prize. The prize question is always some problem which is within the grasp of these pupils as regards its subject matter, but is of such a nature that it requires special ability and is adapted to discovering prospective scholars of real worth. He mentioned that one of tl.e prize winners of earlier years was the well-known Féjer.

2. After discussing limitations on the application of the interpolation process, pointing out the necessity of knowing the function that is satisfied by the given tabular values, referred to as the *underlying* function, and emphasizing the importance of determining the degree of accuracy of the results obtained by interpolation, Professor Reilly indicated the development of the divided difference interpolation formula with a remainder term, in which differences to order n were used, and the remainder after $(n+1)$ terms was expressed in terms of a derivative of order $(n+1)$. The divided difference formula was specialized to produce several of the common formulas, and these in turn were combined to produce others. Thus were found the formulas due to Newton, Gauss, Sterling, Bessel and Everett with the remainder term in each case. The use of the error test in determining the sign and an upper limit of the magnitude of the remainder term was discussed.

To illustrate the use of the remainder terms examples were taken from three tables: (1) a six place table of natural logarithms, (2) a ten place table of common logarithms, and (3) a table of the amounts of a unit at compound interest.

In the first table it was found that (given log 7741 and log 7742) log 7741.5 $=8.954350$, while $R_2=.0021\times10^{-6}$ if, as is commonly done, descending differences and descending factorials are employed. It was also found that (given log 438 and log 439) log $438.5=6.083359$, while $R_2=.65\times10^{-6}$, and that (given log 53 and log 54) log $53.5=3.979638$, while $42.9\times10^{-6}<R_2<44.5\times10^{-6}$ These results indicate that if linear interpolation is to be employed, it is certainly not desirable to print a table of natural logarithms to six places when the corresponding numbers are given to only three figures or two figures.

In the second table it was found that (given log 12153 and log 12154) log $12153.5=4.084\ 7013\ 649$, while $R_2=3.7\times10^{-10}$; also that (given log 95678 and log 95679) log $95678.5=4.980\ 8143\ 581$, while $R_2=.06\times10^{-10}$. This shows that in a common logarithm table where the numbers are given to five figures and the logarithms to ten places linear interpolation is satisfactory in the latter part of the table, but not in the former part, where the use of at least second order differences is necessary.

In the third table, that of the amounts of a unit at compound interest as ordinarily constructed, interpolation was far less satisfactory than in the two other tables considered. It was found that [given $(1.02)^{10}$, $(1.0225)^{10}$, $(1.025)^{10}$, $\cdots$, to seven places] $(1.02125)^{10}=1.2340989$, when linear interpolation was employed, while $-840\times10^{-7}<R_2<-824\times10^{-7}$. Also that $R_3=8\times10^{-7}$, and $R_4=-.09\times10^{-7}$, which shows the need for third order differences. Again [given

$(1.04)^{70}$, $(1.045)^{70}$, $(1.05)^{70}$, $\cdots$, to seven places] it was found necessary to use eleventh order differences to obtain the value of $(1.0525)^{70}$ to seven places.

Two suggestions were made, (a) that shorter intervals in the interest rate be used even if it were thereby necessary to lessen the period of years covered by the table, and (b) that a statement be made in the "Explanation of the Tables" indicating what degree of accuracy is obtainable by interpolating with given orders of differences in various sections of the table.

Meetings of the Board of Trustees

Ten members of the Board of Trustees were present at the Cleveland meeting.

The following forty-one persons and one institution were elected to membership on applications duly certified:

To Individual Membership

Nola Lee Anderson, Ph.D. (Missouri). Chm., Dept. of Math., Sophie Newcomb Coll., New Orleans, La.

Ida M. Baker, A.M. (Columbia). Asso. Prof., School of Educ., Western Reserve Univ., Cleveland, Ohio.

L. M. Bauer, A.B. (Oakland City Coll.). Principal, Wabash Twp. High School, Griffin, Ind.

J. C. Bay. Librarian, The John Crerar Library, Chicago, Ill.

Lois E. Bell, A.M. (Kansas). Teacher, Junior Coll., Independence, Kans.

T. A. Bickerstaff, A.M. (Mississippi). Instr., Univ. of Mississippi, University, Miss.

Archie Blake, B.S. (Chicago). Grad. student, Univ. of Chicago, Chicago, Ill.

Arthur B. Brown, Ph.D. (Harvard). Instr., Columbia Univ., New York, N. Y.

J. H. Bushey, Ph.D. (Michigan). Asst. Prof. of Math. and Insurance, Hunter College, New York, N. Y.

D. D. Butterfield, A.M. (Princeton). Instr., Phillips Exeter Acad., Exeter, N. H.

Laura E. Christman, A.M. (Wisconsin). Teacher, Senn High School, Chicago, Ill.

A. J. Cook, Ph.D. (Chicago). Asso. Prof., Univ. of Alberta, Edmonton, Canada.

Max Coral, M.S. (Chicago). Univ. of Chicago, Chicago, Ill.

Margaret L. Darragh, A.B. (Hanover Coll.). Instr., Roosevelt High School, Chicago, Ill.

Ralph Deutsch, A.M. (Columbia). Teacher, New Utrecht High School, Brooklyn, N. Y.

F. G. Dressel, M.S. (Michigan). Instr., Duke Univ., Durham, N. C.

Sarah Fahnestock, M.S. (Chicago). Head of Dept., Marymount College, Salina, Kans.

C. W. Foard, Ph.D. (Iowa). Prof., Math. and Physics, Youngstown Coll., Youngstown, Ohio.

Pauline F. Folk, A.B., B.E. (Colorado). Grad. student, Univ. of Colorado, Boulder, Colo.

D. H. Frank, B.S. (C. C. N. Y.). Teacher, George Washington High School, New York, N. Y.

F. L. Manning, M.S. (Rutgers). Asst. Prof., Ursinus Coll., Collegeville, Pa.

Sister Mary Joan, A.B. (St. Catherine's Coll.) Teacher, St. Catherine's High School, Racine, Wis.

Dorothy McCoy, Ph.D. Prof., Belhaven Coll., Jackson, Miss.

A. F. Mish, A.B. (West Virginia). Instr., High School, Grafton, West Va.

J. P. Nickol, Ph.D. (Fribourg). Prof., Physics and Math., St. Bonaventure's Coll. St. Bonaventure, N. Y.

C. O. Oakley, Ph.D. (Illinois). Asst. Prof., Brown Univ., Providence, R. I.

A. W. Rankin, Electrical Laboratories, Electric Service Supplies Co., Philadelphia, Pa.

Y. K. Roots, M.S. (New York Univ.) Prof., Math. and Physics, Findlay Coll., Findlay, Ohio.

C. H. Rowe, (Fellow of Trinity Coll., Dublin). Erasmus Smith's Prof. of Math., Univ. of Dublin, Dublin, Ireland.

J. A. SCHOUTEN, Prof. Dr., Technological Univ., Delft, Holland. (Lecturer, 1930–1931 at Harvard, M.I.T., and Princeton.)

C. L. SEARCY, C.E. (Purdue), A.M. (California). Asst. Prof., Univ. of Nevada, Reno, Nev.

C. R. SHERER, A.M. (Nebraska). Head of Dept., Texas Christian Univ., Ft. Worth, Tex.

A. E. STANILAND, A.M. (Pittsburgh). Instr., Univ. of Pittsburgh, Pittsburgh, Pa.

H. E. STELSON, Ph.D. (Univ. of Iowa). Asst. Prof., Kent State Coll., Kent, Ohio.

J. L. SYNGE, Sc.D. (Dublin). Prof., Univ. of Toronto, Toronto, Ont., Canada.

H. B. THORNTON, A.M. (Cincinnati). Head of Dept., Sumner Jr. Coll., Kansas City, Kans.

O. E. Walder, A.M. (Nebraska). Instr., South Dakota State Coll., Brookings, S. Dak.

MAUD WILLEY, A.M. (Mills Coll.). Instr., Alabama Coll., Montevallo, Ala.

ALBERTA WOLFE, M.S. (Iowa State Coll.). Instr., Western Coll. for Women, Oxford, Ohio.

H. M. YARBROUGH, Ph.D. (Indiana). Head of Dept., Western Kentucky State Teachers Coll., Bowling Green, Ky.

B. C. ZIMMERMAN, A.M. (St. Louis Univ.). Grad. student, Marquette Univ., Milwaukee, Wis.

To Institutional Membership

UNIVERSITY OF MAINE, Orono, Maine

The financial report for the year 1930 was presented by the Secretary-Treasurer. It was accepted by the Trustees, subject to the inspection of a subcommittee; on Thursday Professor Slaught for the committee on finance and Professors E. W. Chittenden and C. A. Hutchinson examined the report and the evidences of assets and declared the report satisfactory.

Professor Dunham Jackson, chairman of the Committee on Geometry, presented a report of that committee and the Trustees voted to approve the report which concerns a possible year course in plane and solid geometry, without passing judgment as to the relative merits of any particular type of course. The full report will appear in another place in the MONTHLY.

The Trustees adopted a resolution on the death of Professor Cajori. This is incorporated in the report of the annual business meeting.

The Secretary reported that Presidents Hedrick and Young had made coincident appointment of Professor E. V. Huntington to represent the Society and the Association on the Secondary Committee on Electrical Definitions of the American Standards Association.

It was voted to approve the following associate editors of the MONTHLY for the year 1931:

Elizabeth Carlson	B. F. Finkel	J. R. Musselman
N. A. Court	R. E. Gilman	H. L. Olson
Otto Dunkel	R. A. Johnson	D. E. Smith
H. S. Everett	H. W. Kuhn	F. M. Weida

It was voted to accept the invitation of the University of California at Los Angeles to meet there in conjunction with the Society in the summer of 1932.

The President and Secretary were authorized to do whatever seems desirable in the way of formal participation by the Association in the latter part of the S.P.E.E. summer school at Minneapolis next summer. It is probable that an

evening program will be held on the last Friday of the S.P.E.E. meeting and immediately before the meetings of the Mathematical Association.

Annual Business Meeting of the Association

The Secretary announced the names of those elected to membership. He reported also the deaths of the following members:

C. W. Andrews, Librarian emeritus, The John Crerar Library, Chicago, Ill. (November 20, 1930).

W. O. Beal, Chairman, Dept. of Astronomy, University of Minnesota (February 15, 1930).

G. C. Bordner, Professor of mathematics, State Teachers College, Kutztown, Pa. (May 15, 1930).

William Cain, Emeritus Professor of mathematics, University of North Carolina (December 6, 1930).

Florian Cajori, Emeritus Professor of the history of mathematics, University of California (August 14, 1930).

Mary E. Caster, Teacher of mathematics, Eastside High School, Paterson, N. J. (December 7, 1930).

Major C. H. Chepmell, of Bristol, England (November 18, 1930).

C. W. Crum, M.D., Baltimore, Md. (December 20, 1929).

J. O. Eckersley, Chief engineer, Dept. of Markets, New York City (November 11, 1930).

J. L. Markley, Professor of mathematics, University of Michigan (April 20, 1930).

E. B. Morris, Actuary, Travelers Insurance Co., Hartford, Conn. (December 19, 1929).

E. A. Pattengill, Associate professor of mathematics, Iowa State College (February 10, 1930).

R. E. Peterson, Dept. of mathematics, Pennsylvania State College (Summer, 1929).

R. A. Sheets, Associate professor of mathematics, Denison University (December 3, 1930).

J. M. Taylor, Emeritus professor of mathematics, Colgate University (July 31, 1930). (Charter member of M.A.A., resigned 1920).

H. E. Trefethen, Associate professor of mathematics and astronomy, Colby College (November 3, 1930).

The election of officers for the year 1931 resulted in the following, as reported by the tellers, Professors C. A. Hutchinson and C. H. Yeaton:

For President: E. T. Bell, 330 votes; W. C. Graustein, 255 votes.

For Vice-Presidents: Arnold Dresden, 396 votes; Tomlinson Fort, 231 votes; C. N. Moore, 305 votes; W. H. Roever, 205 votes.

For additional members of the Board of Trustees, to serve until January 1934: C. C. Camp, 218 votes; L. L. Dines, 335 votes; T. C. Fry, 382 votes; J. W.

Glover, 285 votes; F. L. Griffin, 248 votes; H. W. Kuhn, 244 votes; E. P. Lane, 318 votes; H. P. Manning, 262 votes.

The following were accordingly declared elected:

President: E. T. BELL, California Institute of Technology.

Vice-Presidents: ARNOLD DRESDEN, Swarthmore College, C. N. MOORE, University of Cincinnati.

Additional members of the Board of Trustees: L. L. DINES, University of Saskatchewan; T. C. FRY, Bell Telephone Laboratories; J. W. GLOVER, Teachers Insurance and Annuity Association; E. P. LANE, University of Chicago.

The following resolution, presented to the Trustees on Wednesday by Professor Lao G. Simons, was also presented at this meeting of the Association and adopted by rising vote:

WHEREAS: Our fellow member and Trustee, Florian Cajori, has passed away from the scene of his earthly labors;

AND WHEREAS: Professor Cajori was a Charter Member of the Mathematical Association of America and was also its President in 1917;

AND WE RECOGNIZE FURTHER: That his professional connections with great universities and his unique position as Professor Emeritus of the History of Mathematics caused him to exert an unusual influence on the body of American students;

That his active association with many learned societies, on the programs of whose meetings his name appeared at frequent intervals, made known the extent of his scholarship and the charm of his personality to a wide circle of men and women;

That his extended publications on a remarkable variety of subjects within the compass of the History of Science constitute an almost inexhaustible fund of reference material for the student and teacher:

BE IT RESOLVED: That we, the Trustees and members of the Mathematical Association of America, put on record our appreciation of the contributions of Professor Cajori to his chosen field, the History of Mathematics, and the part that he played in making known internationally the researches of American scholars.

REPORT OF THE SECRETARY-TREASURER AS TREASURER, DECEMBER 15, 1930

RECEIPTS		EXPENDITURES		
Balance Dec. 16, 1929	$11,221.38	Publisher's bills (Nov. '29–Oct. '30)		$5,105.05
1928 indiv. dues	29.25	President's office		52.76
1929 indiv. dues	359.20	Manager's office		30.91
1929 instit. dues	26.50	Editor-in-chief's office		517.92
1930 indiv. dues	6,500.23	Other editors' postage		5.00
1930 instit. dues	821.50	Committee on Geometry		68.49
1930 subscriptions	830.82	*Register*		542.12
Initiation fees	226.00	Secretary-Treasurer's office:		
Advertising	718.82	Postage	$337.89	
Sale *Register*	6.50	Bond	5.00	
Sale copies of MONTHLY	246.21	Safety deposit	4.00	
Sale First Carus Mon.	45.00	Office supplies	89.10	
Sale Second Carus Mon.	45.00	Express, tel., etc.	59.50	
Sale Third Carus Mon.	32.50	Ins. back copies of MONTHLY	11.00	
Sale Fourth Carus Mon.	1,025.00	Clerical work	1,705.63	
Advance sale Carus Mon.	1.25	Printing	275.95	
Fee for translation rights Carus Mon.	1.00	Library expense	223.85	

Sale Rhind Papyrus	1,545.00	
Carrying charges Papyrus	88.50	
Contributions A. B. Chace	2,375.18	
Int. Oberlin Savgs. Bk.	111.23	
Int. Peoples Bkg. Co.	103.64	
Int. Liberty Bonds	85.00	
Int. Hardy Fund	120.00	
Int. certifs. of deposit	42.34	
Int. from Genl. Endowment Fund Bonds	385.00	
Int. Chace Fund	91.25	
Int. Chauvenet Fund	25.00	
Int. from investment of current funds	150.00	16,036.92
Total 1930 receipts		$27,258.30

Paid copies MONTHLY	50.19	
Des Moines meeting	90.00	
Providence meeting	82.12	
Cleveland meeting	6.00	
Refund 1930 subscription	3.60	
Paid members' *Annals*	5.00	
Typewriter	63.03	3,011.86
Annals subvention		225.00
Paid to sections from initiation fees		166.45
Transferred to Genl. Endowment		3,000.00
Cost above par of new bonds for Genl. Endowment Fund plus accrued int.		110.50
Paid B. F. Finkel int. Hardy Fund		120.00
Sustaining memb. in Amer. Math. Society		100.00
Printing Rhind Papyrus		2,375.18
Carrying charges Papyrus		124.40
Expense acct. Papyrus		36.02
Expense acct. *Bibl. Math.*		50.00
Expense acct. Carus Mons.		131.45
Award Chauvenet Prize		100.00
Honorarium Fourth Carus Mon.		300.00
Transfer to Chace Fund		1,575.76
Transfer to Carus Mon. Fund		1,004.28
Total expenditures		$18,753.15

Total expenditures	18,753.15	
Balance to the end of 1930 business	8,505.15	
Received on 1931 business	731.50	
Book balance Dec. 15, 1930	$9,236.65	

Cash on hand	12.53
Checking account	268.41
Oberlin Savgs. Bk. acct.	2,457.00
Peoples Bkg. Co. acct.	2,021.81
Liberty Bonds	1,000.00
Iowa Ry & Light Co. 5% Bonds	3,000.00
Certif. of deposit	476.90
Bank balance Dec. 15, 1930	$9,236.65

EXHIBIT OF THE FUNDS OF THE ASSOCIATION

CHAUVENET PRIZE FUND

Balance Dec. 16, 1929		$605.00
Interest	$25.00	
Amount set aside for 1930	20.00	45.00
		$650.00
Award Dec. 1929		100.00
		$550.00
Iowa Rwy & Light Co. 5% Bond	$500.00	
Cash in bank	50.00	
Balance Dec. 15, 1930		$550.00

Carus Monograph Fund

Balance Dec. 16, 1929		$4,560.89
Receipts: Sales	$1,148.75	
Interest	182.28	1,331.03
		$5,891.92
Expenditures	131.45	
Accrued interest on new bond	4.28	135.73
		$5,756.19
Certificates of deposit	$4,693.17	
Cleveland Trust Securities Co. Gold Bond	1,000.00	
Cash in bank	63.02	
Balance Dec. 15, 1930		$5,756.19

Arnold Buffum Chace Fund

Balance Dec. 16, 1929		$1,416.00
Receipts: Sales	$1,545.00	
For carrying charges	88.50	
Interest	105.26	1,738.76
		$3,154.76
Expenditures: Expense acct. Rhind Papyrus	24.59	
Premium on bond and accrued int.	75.76	
For carrying charges	124.40	224.75
		$2,930.01
Iowa Rwy & Light Co. 5% Bond	$1,000.00	
Western United Gas and Elec Co. Bond	1,500.00	
Certificate of deposit	430.01	
Balance Dec. 15, 1930		$2,930.01

Life Membership Fund

Liability on life memberships Dec. 16, 1929	$459.20
To be transferred to current funds, surplus	12.89
Liability on life memberships as of Jan. 1, 1931	$446.31

General Endowment Fund

Balance Dec. 16, 1929		$5,000.00
Transferred from current funds in 1930		3,000.00
		$8,000.00
Liberty Bond	$1,000.00	
Land Trust Certificate	1,000.00	
Cleveland Trust Investment Co. Gold Bond	1,000.00	
Idaho Power Co. 5% bonds	2,000.00	
Northwestern Elec Co. Bonds	3,000.00	
Balance Dec. 15, 1930		$8,000.00

Of the funds on hand, indicated in the first division of the financial report, $63.02 belongs to the Carus Monograph Fund (not yet transferred); $50.00 belongs to the Chauvenet Prize Fund; and $446.31 is held as a Life Membership Fund, representing the liability on life memberships already paid for, as of date Jan. 1, 1931. Aside from these amounts, the Carus Monograph Fund, to the amount of $4,693.17, is carried as a separate fund in the form of two certificates of deposit which bear 4%, compounded quarterly; $430.01 of the Arnold Buffum Chace Fund is similarly carried in the form of a certificate of deposit; the contribution of Professor Walter B. Ford to the Chauvenet Fund is carried as a 5% Gold Bond; and the sum of $8,000.00 is held in reserve as the General Endowment Fund, in securities as listed above.

When the accounts were closed Dec. 15, 1930, there remained on the total business for the year 1930 the following items:

Bills Receivable (partly estimated)	
1930 individual dues	$200.00
Advertising	100.00
	$300.00

Bills Payable (partly estimated)	
Publisher's bills (Nov., Dec. 1930)	$1,150.00
President's office	70.00
Manager's office	20.00
Editor-in-chief's office	110.00
Other editors' postage	40.00
Secretary-Treasurer's office	350.00
Annals subvention	75.00
Initiation fees due to sections	750.00
Carus Monograph Fund	63.02
Chauvenet Prize Fund	50.00
Life Membership Fund	446.31
Printing catalog of library	400.00
	$3,524.33

If to the balance on 1930 business shown in the report, $8,505.15, there be added the bills receivable, $300.00, and there be subtracted the estimated bills payable, $3,524.33, there results an estimated final balance on 1930 business of approximately $5,280, which represents the accumulated surplus in current funds. This is a gratifying result for the year when compared with the corresponding figure of $6,400 of a year ago, for it will also be kept in mind that $3,000 was transferred from the current funds to the General Endowment Funds by recommendation of the Executive Committee and vote of the Trustees.

W. D. Cairns, *Secretary-Treasurer*

CONCERNING CERTAIN LINEAR TRANSFORMATION APPARATUS OF CRYPTOGRAPHY[1]

By LESTER S. HILL, Hunter College

1. *Introductory Note*

Of especial interest in systematic cryptography is the linear transformation:

$$(T)\qquad \begin{aligned} y_1 &= a_{11}x_1 + a_{12}x_2 + \cdots + a_{1f}x_f + a_1, \\ y_2 &= a_{21}x_1 + a_{22}x_2 + \cdots + a_{2f}x_f + a_2, \\ &\cdots\cdots\cdots\cdots\cdots\cdots \\ y_f &= a_{f1}x_1 + a_{f2}x_2 + \cdots + a_{ff}x_f + a_f, \end{aligned}$$

in which f is any positive integer, and the variables x_i, y_i, as well as the coefficients a_{ij} and a_i are elements of an arbitrary field, finite or infinite. But the linear apparatus which may be profitably employed is much more extensive. To meet the demands of effective cipher construction, we must often operate in sets which do not possess full field character. The necessary operational sets are really special linear associative and commutative algebras. In the present paper, we shall call these sets *scales*. For our purposes, the transformation T must be made available in any scale.

Moreover, it is highly desirable to extend the transformation T in the sense of permitting the x_i, y_i, a_{ij}, a_i to be square matrices of arbitrary order in an arbitrary scale. This enables us to convert a sequence $x_1, x_2, \cdots, x_f$ of f matrices into another sequence $y_1, y_2, \cdots, y_f$ of f matrices. The specification of conditions under which a unique inverse transformation exists will naturally be important.

When the underlying scale is of the type of most immediate cryptographic significance, namely the type $S(n)$ discussed in Section 3, the linear transformations T may be effected with extraordinary speed and accuracy by means of a mechanical device, no calculations of any sort being required. To avoid the expense of preparing machines of different structures, one for encipherment and the other for decipherment, we employ *involutory* transformations of type T(that is to say, transformations of period 2).

It is hoped that these notes will direct attention to a fascinating, although sadly neglected, domain of applied algebra.

2. *Scales*

The word *ring*[2] has been quite generally adopted to describe any finite or infinite set R, over which operations of so-called "addition" and "multiplica-

[1] *A Note by the Editor*: This paper was presented under a different title to the American Mathematical Society at Boulder, Colorado in August, 1929. It is the second article by Professor Hill on the subject of *Cryptography* to be published in this Monthly. The first one was *Cryptography in an algebraic alphabet*, in vol. 36 (1929), pp. 306–312.

[2] See Hasse, *Höhere Algebra*, Part 1, pp. 7–9.

tion" are in any way uniquely specified, provided that: (1) R contains at least two different elements; (2) multiplication is distributive with respect to addition, and each of these two operations is associative and commutative; and (3) if α and β denote elements of R, not necessarily different, then R contains exactly one element γ such that $\alpha+\gamma=\beta$.[3]

It is readily shown that any ring R contains exactly one zero element, and we shall denote this element by 0. The zero element has the properties, the first of which is definitional and pertains only to this element, that $\alpha+0=\alpha$ and $\alpha\cdot 0=0$, where α denotes any element of R. Concerning the second of these properties, we note that there is an infinity of rings in which every product vanishes (is equal to the zero element). According to the definition given below, such rings are clearly not *scales*.

Each element α of any ring determines uniquely an element δ such that $\alpha+\delta=0$, and δ is called the "negative" of α. We write $\delta=-\alpha$, noting the obvious implication that $\alpha=-\delta$. The element γ of postulate (3) above is denoted by $\beta-\alpha$; and we observe that $\beta-\alpha=\beta+(-\alpha)$.

Let α, β, γ denote elements, not necessarily different, of a ring R. We easily see that $\alpha(-\beta)=(-\alpha)\beta=-\alpha\beta$, $(-\alpha)(-\beta)=\alpha\beta$, $\alpha(\beta-\gamma)=\alpha\beta-\alpha\gamma$; and also that each of the equations $\alpha=\beta$, $\alpha-\beta=0$, implies the other.

An element α of a ring R is a "divisor of zero" if R contains an element β different from zero ($\beta\neq 0$) such that $\alpha\beta=0$. The zero element of a ring is always a divisor of zero.

By reason of the commutativity of multiplication, a ring R can not contain more than one element ϵ such that $\epsilon\alpha=\alpha$ for every element α of R. If one such element ϵ is present, it is called the *unit element* of R, and may be conveniently denoted by 1.

In all that follows, we shall operate exclusively in those rings which we distinguish as *scales*. Hence we emphasize the definition: *A scale is a ring which contains a unit element.* If a ring R is a scale, we shall ordinarily denote it by the letter S.

Let α denote any element of a scale S. It is readily established that S can not contain more than one element β such that $\alpha\beta=1$. If one such element β is present in the scale, we call it the "reciprocal" of α, writing $\beta=1/\alpha$, and noting the implication that $\alpha=1/\beta$. An element of a scale will be classed as *regular* or *singular* according as it has, or has not, a reciprocal.

In any scale, the unit and zero elements are respectively regular and singular; and the product of two elements, not necessarily different, is regular when and only when both elements are regular. The negative and the reciprocal of a regular element are regular. *A field is a scale in which the zero is the only singular element.*

[3] When no misunderstanding can arise, we shall employ without comment the familiar terminology and notations of elementary algebra. Thus, for instance, we shall say that addition and multiplication of the elements α and β of a ring yield respectively the "sum" $\alpha+\beta$ and the "product" $\alpha\beta$.

A regular element of a scale is never a divisor of zero. In some scales, every singular element is a divisor of zero; in other scales, this is not the case.

If α is any element, and β any regular element, of a scale S, then S contains exactly one element, γ, such that $\beta\gamma=\alpha$. We write $\gamma=\alpha/\beta$, observing that, in fact, $\alpha/\beta=\alpha(1/\beta)$.

Exponential notations are easily introduced. If α is any element of a scale S, the meaning of the symbol α^n, for positive integral n, requires no comment. When n is a negative integer or zero, this symbol is defined only for the case in which α is a *regular* element of S, and the specifications in that case are: $\alpha^0=1$ (the unit element of S), $\alpha^n=(1/\alpha)^{-n}$.

It should be noted that every field is a scale, and that every scale is a ring. The following two sections will furnish examples of scales which are fields, and of scales which are not fields. There exist an infinity of rings (finite rings as well as infinite rings) which are not scales; but the present paper completely disregards such rings.

3. *Simple Examples of Scales*

It is evident that the fields of rational, real, and ordinary complex numbers furnish three examples of scales. A subscale of each of these is found in the set of all positive and negative integers and zero. This infinite subscale contains only two regular elements, namely ± 1, and only one divisor of zero, namely 0.

Of exceptional practical interest in cryptography are the finite modular scales which we here designate as of type $S(n)$. For the integer $n\geqq 2$, let $S(n)$ denote any set of n elements associated, one-to-one, with the n integers $0, 1, 2, \cdots, n-1$. If the elements α, β of $S(n)$ are associated with the integers a, b, we define:

$$\alpha+\beta=\gamma,\quad \alpha\beta=\delta$$

where γ and δ are the elements of $S(n)$ associated respectively with the *remainders* obtained upon dividing, by n, the ordinary sum $a+b$, and the ordinary product ab, of integers.

With operations thus defined, modulo n, we see that $S(n)$ is a finite scale. Its regular elements are those associated with integers prime to n. When n is prime, $S(n)$ is a field.

It will be convenient to treat, as the elements of $S(n)$, the n integers $0, 1, 2, \cdots, n-1$ themselves, regarded as mere marks or symbols.

For cipher construction, perhaps the most useful scales of the type $S(n)$ are those which correspond to $n=23, 25, 26, 27, 36, 100, 101$. The first and the last of these seven are, of course, fields.

We shall draw our illustrative material from $S(26)$. We tabulate here, for later reference, the regular elements of this scale, together with their reciprocals:

$S(26)$

Element:	1,	3,	5,	7,	9,	11,	15,	17,	19,	21,	23,	25
Reciprocal:	1,	9,	21,	15,	3,	19,	7,	23,	11,	5,	17,	25

The negative of the reciprocal of an element in any scale is the reciprocal of the negative. Thus we have here:

$$-21=1/(-5)=1/21=5;\quad -17=1/(-23)=1/3=9;\ \text{etc.}$$

Operations in $S(26)$ may be further illustrated as follows: $3+11=14$; $17+12=3$; $9+17=0$, whence $-9=17$ and $-17=9$; $3(7)=21$, whence $21/3=7$ and[4] $21/7=3$; $7(15)=1$, whence $1/7=15$ and $1/15=7$; etc. The negative of any element is obvious: $-0=0$, $-1=25$, $-2=24$, $-3=23$, etc.

4. *Scales Obtained by Algebraic Extension of Other Scales*

The theory of polynomials in any *field* is so familiar a chapter of modern algebra that not very much needs to be said here concerning polynomials in an arbitrary *scale* S (polynomials with "coefficients" which are elements of S). We note only a few points of special interest. A polynomial in a scale S is conveniently distinguished as *primary* if the coefficient in the term of highest "degree" is a *regular* element of S. Each element α of S is regarded as a polynomial in S, degrees being as follows: (1) when $\alpha\neq 0$, it is a polynomial of degree zero; and (2) when $\alpha=0$, it is a polynomial of degree[5] -1. Regular and singular elements of S, regarded as polynomials in S, are classed respectively as primary and non-primary.

We note that the degree of the product of two polynomials in a scale is equal to the sum of their degrees whenever at least one of the polynomials is primary and the other is not the polynomial 0 (of degree -1). We record also this fundamental *division property*:

Let S be any scale, finite or infinite. Let P denote any polynomial, and D any *primary* polynomial, in S. There are uniquely determined two polynomials Q and R in S, the latter of degree less than the degree of D, such that $P=QD+R$.

It is convenient to designate R as the *residue of* P, *modulo* D; and to write: $R=\text{Res}\ (P, \text{mod}\ D)$. If the degree of P is less than that of D, we see at once that[6] $\text{Res}\ (P, \text{mod}\ D)=P$.

Let us now select, as a modulus, any polynomial N, in S, which is primary and of degree $n\geqq 2$. It is easy to define addition and multiplication over the set U of all polynomials in S which have degrees less than n, *in such manner that* U *will be closed under these operations and will constitute a scale.* We need merely specify,[7] as the sum of two polynomials A, B of U, the sum $A+B$ in S;

[4] Similarly since $17(18)=20$ we might expect to have $20/17=18$ and $20/18=17$; but such is not the case, for while $17(18)=20$ implies $20/17=18$, it does not imply $20/18=17$. The element 18 is singular, and $20/18$ is not defined.

[5] Any other negative real number would serve equally well, for our purposes, to mark the degree of the polynomial 0. We wish merely to signalize that the "degree" of this polynomial is to be regarded as less than that of any other polynomial in S.

[6] In this case, Q is the polynomial 0, and $R=P$.

[7] For the case in which the scale S is a field, this procedure is very familiar. In this case, every polynomial in S, except the polynomial 0, is primary. But to obtain a scale U which is a field, we must employ, as modulus N, a primary polynomial *irreducible* in the field S.

and as the product, the polynomial Res $(AB, \text{mod } N)$, where AB is the product in S.

The scale U plainly contains a subset V which is a scale simply isomorphic with the scale S. The scale V consists of those polynomials of U each of which is represented by an element of S. In this sense, we may regard U as an *extension* of S.

It is evident that when the scale S is finite, consisting of k elements, the scale U will likewise be finite, consisting of k^n elements, where n is the degree of the modulus N.

For the benefit of those readers who may not be experienced in manipulations of the character here considered, we append two examples.

Example 1: Let $S=S(2)$, of which the elements[8] are 0 and 1. Let $N=x^2+x+1$. The elements of U are the four polynomials 0, 1, x, $x+1$ in $S(2)$. Denoting these elements by a, b, c, d respectively, we find that:

$$c + d = x + (x + 1) = 1 = b; \quad cd = \text{Res } (x^2 + x, \text{ mod } N) = 1 = b; \text{ etc.}$$

Since, in this case, S is a field, and N is irreducible in S, the scale U is a field. Its operation tables in full are:

Addition

	a	b	c	d
a	a	b	c	d
b	b	a	d	c
c	c	d	a	b
d	d	c	b	a

Multiplication

	a	b	c	d
a	a	a	a	a
b	a	b	c	d
c	a	c	d	b
d	a	d	b	c

The zero element is a, and the unit element is b. Every element is its own negative.[9]

For variety, let us select a modulus which is reducible in $S(2)$, say $N'=x^2+1$. We are led to a scale U', the operation tables of which, aside from the four products, $cc=b$, $cd=dc=d$, $dd=a$, are exactly the same as those of U. The zero and unit elements are again a and b, respectively. There is a singular element other than the zero, namely d, and U' is therefore not a field.

Example 2: Let $S=S(6)$, of which the six elements are:

$$0; \ 1 = -5; \ 2 = -4; \ 3 = -3; \ 4 = -2; \ 5 = -1.$$

In this case, S is not a field; it contains the four singular elements, 0, 2, 3, 4.

For adequate illustration, we employ three moduli $N_1=x^2-1$, $N_2=x^2-2$, $N_3=x^2-x-1$, leading to the three scales U_1, U_2, U_3, respectively. The elements of each of these scales are the thirty-six polynomials $\alpha+\beta x$ in $S(6)$, where α and β denote any elements of $S(6)$. Interesting light is thrown upon the structural

[8] See Section 3, above. We shall take, as the elements of $S(n)$, the n integers $0, 1, 2, \cdots, n-1$ themselves, adding and multiplying modulo n.

[9] This is true in $S(2)$, and in every scale obtained from $S(2)$ by algebraic extension.

relations of U_1, U_2, U_3 by the following table, which exhibits the reciprocals of all regular elements. For convenience of tabulation, $\alpha+\beta x$ is compactly indicated by[10] $\alpha\beta$.

TABLE

Element	00	10	20	30	40	50	01	11	21	31	41	51
Recip. in U_1		10				50	01					
Recip. in U_2		10				50		51				11
Recip. in U_3		10				50	51	25	31	21	55	01
Element	02	12	22	32	42	52	03	13	23	33	43	53
Recip. in U_1				32					23		43	
Recip. in U_2		52		34		12		13				53
Recip. in U_3		32		12		14		43	53		13	23
Element	04	14	24	34	44	54	05	15	25	35	45	55
Recip. in U_1				34								
Recip. in U_2		54		32		14		55				15
Recip. in U_3		52		54		34	15	05	11	45	35	41

The table is easily interpreted. Thus, for example, it shows at a glance that the element $4+2x$ is singular in each of the three scales U_1, U_2, U_3; and that the element $5+2x$ is singular in U_1, but regular in U_2 and U_3 (with the reciprocals $1+2x$ and $1+4x$, respectively). The scales U_1, U_2, U_3, although of the same order,[11] are of very different structures; in fact, they contain respectively *seven*, *fourteen*, and *twenty-four regular* elements.

From the standpoint of cryptanalysis, it is especially significant that finite scales of the same order r and of widely divergent structures may be so easily specified in this manner.[12] Two finite *fields* of the same order are well known to be algebraically identical. The present section will serve to emphasize that there is an infinity of finite *scales* in which order does not completely determine structure.

5. *Rational Manipulations in a Scale*

It is very readily argued that, with only minor and obvious reservations, all the rational operations and apparatus incidental to the solution, when unique solutions exist, of systems of linear equations in a field are applicable in any scale.

We are especially interested in noting the existence, in any scale, of a full matric algebra of familiar type. The following comments on determinants and matrices in an arbitrary (finite or infinite) scale will not be amiss.

---

[10] The reader will hardly confuse the symbol $\alpha\beta$, used only in the present example, with the product $\alpha\beta$ of elements of $S(6)$.

[11] By the "order" of a finite scale, we understand the number of elements contained in the scale.

[12] When $r=k^n$, with k and n positive integers each greater than 1.

The determinant

$$L = \begin{vmatrix} a_{11} & a_{12} \cdots a_{1n} \\ \cdot & \cdot \quad \cdots \\ \cdot & \cdot \quad \cdots \\ \cdot & \cdot \quad \cdots \\ a_{n1} & a_{n2} \cdots a_{nn} \end{vmatrix},$$

of order n, in which the a_{ij} denote elements of the scale S, has the same meaning and properties as if S were a field. We define L to be *regular* or *singular* according as its "value" is a regular or a singular element of S, where its "value" is fixed by any one of the $2n$ equal expressions in S,

$$\sum_{i=1}^{n} a_{ij}A_{ij}, \qquad \sum_{j=1}^{n} a_{ij}A_{ij}, \qquad i, j = 1, 2, \cdots, n,$$

in which A_{ij} denotes the cofactor (algebraic complement) of a_{ij} in L.

Moreover, L is called the determinant of the square matrix

$$M = \begin{pmatrix} a_{11} & a_{12} \cdots a_{1n} \\ \cdot & \cdot \quad \cdots \\ \cdot & \cdot \quad \cdots \\ \cdot & \cdot \quad \cdots \\ a_{n1} & a_{n2} \cdots a_{nn} \end{pmatrix} = (a_{ij})$$

of order n in S; and M is classed as *regular* or *singular* with L.

Upon occasion, we shall regard each element of the scale S as a matrix of order $n=1$ in S. The set, $SR\{n\}$, of all square matrices of order n in S will be called a *range* of matrices in S. When no misunderstanding can arise concerning the scale S employed, the range of order n in S will be denoted simply by $R\{n\}$. It is clear that $R\{1\}$ consists of all elements of the scale S regarded as matrices of the first order in S.

When $n>1$, a non-commutative algebra may be set up in the range $R\{n\}$ of the scale S. The procedure is a very familiar one,[13] but may be briefly recalled here:

(1) If $A=(a_{ij})$ and $B=(b_{ij})$ are matrices of the range $R\{n\}$ in the scale S, we define $A=B$ when and only when $a_{ij}=b_{ij}$ in S for every pair of indices i, j; and we define addition and multiplication as follows, operations affecting elements a_{ij}, b_{ij}, c_{ij} of S being performed, of course, under the rules of S:

$$A + B = (a_{ij}) + (b_{ij}) = C = (c_{ij}), \text{ with } c_{ij} = a_{ij} + b_{ij}.$$

$$AB = (a_{ij})(b_{ij}) = D = (d_{ij}), \text{ with } d_{ij} = \sum_{q=1}^{n} a_{iq}b_{qj}.$$

[13] The procedure is familiar for the case in which the scale S is a field. When S is not a field, certain precautions must be taken, as will be indicated.

From these definitions it is easy to conclude that, if A, B, C are any matrices of the range $R\{n\}$,

$$A + B = B + A, \quad A + (B + C) = (A + B) + C,$$
$$A(BC) = (AB)C, \qquad A(B + C) = AB + AC.$$

But, in general, $AB \neq BA$.

(2) Let β be any element of the scale S. That matrix of the range $R\{n\}$ in S which has the scalar β in each place of the principal diagonal, and the scalar 0 everywhere else, may be called the *scalar matrix* of β, and may conveniently be denoted by β_n.

(3) If A is any matrix of $R\{n\}$ in S, and β is any scalar in S, each of the mixed products βA and $A\beta$ is defined to be the matrix obtained upon multiplying every element of A by β. It is evident that

$$\beta A = \beta_n A = A\beta_n = A\beta.$$

(4) The range $R\{n\}$ in S contains an unique *zero matrix* 0_n, and an unique *unit matrix* 1_n, such that if A is any matrix of the range,

$$A + 0_n = A, \quad A0_n = 0_n A = 0_n, \quad A1_n = 1_n A = A.$$

These special matrices are merely the scalar matrices of the scalars 0 and 1.

(5) Corresponding to any matrix A of $R\{n\}$ in S, there is exactly one matrix $B = -A$ such that $A + B = 0_n$. The matrix, $-A$, is the mixed product of the matrix A and the scalar -1.

(6) Corresponding to any matrices A and B of the range $R\{n\}$ in S, there is exactly one matrix $C = B - A$ of the range such that $A + C = B$. Clearly, $B - A = B + (-A)$.

(7) If the matrix A of $R\{n\}$ in S is *regular*, there is exactly one matrix B of the range such that $AB = 1_n$; and B also satisfies the equation $BA = 1_n$. We call B the *reciprocal* of A, and write $B = A^{-1}$. If $B = A^{-1}$, then also $A = B^{-1}$.

(8) Let the matrix A of the range $R\{n\}$ in S be *regular*, and let M be any matrix of the range. Then $R\{n\}$ contains exactly one matrix H, and exactly one matrix K, such that $AH = M = KA$. In fact, it is clear that $H = A^{-1}M$ while $K = MA^{-1}$.

(9) The reciprocal of the *regular* matrix $A = (a_{ij})$ of $R\{n\}$ in S is easily written out; it is simply:

$$A^{-1} = \begin{pmatrix} \frac{A_{11}}{\rho} & \cdots & \frac{A_{n1}}{\rho} \\ \cdot & \cdots & \cdot \\ \cdot & \cdots & \cdot \\ \frac{A_{1n}}{\rho} & \cdots & \frac{A_{nn}}{\rho} \end{pmatrix} = \frac{1}{\rho} \begin{pmatrix} A_{11} \cdots A_{n1} \\ \cdot \quad \cdots \quad \cdot \\ \cdot \quad \cdots \quad \cdot \\ A_{1n} \cdots A_{nn} \end{pmatrix},$$

where A_{ij} is the cofactor of a_{ij} in the determinant of A, and ρ is the value of that determinant as worked out in the scale S. A singular matrix has no reciprocal.

(10) If we agree to interpret the mixed sum $\beta+A=A+\beta$, where β is a scalar in S and A is a matrix of the range $R\{n\}$ in S, as the sum $\beta_n+A=A+\beta_n$ of matrices of $R\{n\}$, then in any expression like

$$c+\sum_{q=1}^{m}a_qx_q,$$

where c, a_q, x_q are matrices of $R\{n\}$, we may replace any scalar matrix by its corresponding scalar.

(11) Exponential notations will be self-explanatory. We note, however, that the symbol A^{-q}, where A is a matrix of the range $R\{n\}$ in the scale S, and q is a positive integer or zero, is not defined unless A is regular. When A is regular, $A^0=1_n$, $A^{-q}=(A^{-1})^q$.

We are now prepared to discuss a novel class of ciphers associated with the general linear transformation in the general range $R\{n\}$ of the general scale S. It will be necessary, of course, to employ only such transformations as have unique inverses. Also it will be very desirable, for practical reasons, to make easily available a large class of *involutory* transformations.

6. *Linear Transformations in the General Range*

Consider the linear transformation T_a:

$$\begin{aligned}
y_1 &= a_{11}x_1+a_{12}x_2+\cdots+a_{1f}x_f+a_1,\\
&\cdots\cdots\cdots\cdots\cdots\\
y_f &= a_{f1}x_1+a_{f2}x_2+\cdots+a_{ff}x_f+a_f,
\end{aligned}$$

where f is any positive integer, and the x_i, y_i, a_{ij}, a_i are matrices of any range $R\{n\}$ in any scale S. All operations required to effect this transformation are to be performed in the range $R\{n\}$.

If $n>1$, the algebra of $R\{n\}$ is non-commutative, as explained in Section 5. The range $R\{1\}$ coincides with the scale S itself, and the algebra of this range with the (commutative) algebra of S. When $n=1$, it is clear that T_a is merely a scalar transformation, the variables and the coefficients being elements of the scale S.

In all that follows, we shall understand the range $R\{n\}$ to include the underlying scale S as the special range $R\{1\}$. The transformation T_a converts a sequence of f matrices of the general range $R\{n\}$ into another such sequence. But when $n=1$, the matrices are of order 1, and are therefore merely *scalars* (elements of the scale S).

The rectangular array of $f(f+1)$ matrices,

$$P_a = \begin{bmatrix} a_{11} \cdots a_{1f} & a_1 \\ \cdot \quad \cdots \quad \cdot & \cdot \\ \cdot \quad \cdots \quad \cdot & \cdot \\ a_{f1} \cdots a_{ff} & a_f \end{bmatrix},$$

will be called the *schedule* of T_a, and will be designated as $P_a = [(a_{ij}), a_i]$. The square array of f^2 matrices $M_a = (a_{ij})$ will be called the *basis* of T_a.

We denote by J the set of all transformations which can be obtained in this way, for a fixed integer f, from the range $R\{n\}$ in the scale S. Let T_a, with $P_a = [(a_{ij}), a_i]$, and T_b, with $P_b = [(b_{ij}), b_i]$, be two transformations of the set J. Applying T_a to a sequence of f matrices $x_1, x_2, \cdots, x_f$ of $R\{n\}$ in S, we obtain the sequence $y_1, y_2, \cdots, y_f$ of matrices of the same range; applying T_b to the sequence $y_1, y_2, \cdots, y_f$, we obtain the sequence $z_1, z_2, \cdots, z_f$; compactly: $T_a(x) = y$, $T_b(y) = z$. The set J evidently contains an unique transformation T_c, with $P_c = [(c_{ij}), c_i]$, such that $T_c(x) = z$. We say that T_c is the *product* $T_b T_a$, distinguishing this product from $T_a T_b$. It is quickly found that

$$(1) \qquad c_{ij} = \sum_{q=1}^{f} b_{iq} a_{qj}, \quad c_i = b_i + \sum_{q=1}^{f} b_{iq} a_q,$$

the operations required for calculation by these formulas being effected according to the algebra of the range $R\{n\}$.

It is readily shown that products of transformations in J are associative; if T_a, T_b, T_c are any transformations in J, then $T_a(T_b T_c) = (T_a T_b) T_c$.

7. *A Fundamental Lemma*

Let T_a, with the schedule $P_a = [(a_{ij}), a_i]$, be a transformation belonging to the set J considered in Section 6. We fix our attention upon the *basis* $M_a = [a_{ij}]$ of T_a. If parentheses are removed from all the f^2 matrices in the square array $[a_{ij}]$, there results a square matrix G_a in the scale S, of order $g = fn$. The matrix G_a will be called the *frame matrix* of T_a. It is evident that G_a belongs to the range $R\{g\}$ in the scale S.

The following lemma is fundamental. It may be established by a straightforward argument which will be omitted here.

Lemma: Let T_a, T_b, T_c be transformations in J; and let their frame matrices be G_a, G_b, G_c respectively. Then $G_c = G_a G_b$ if[14] $T_c = T_a T_b$. In other words, *the frame matrix of a product of transformations is the corresponding product of the frame matrices of the transformations.*

8. *Regular Transformations in J.*

We consider now the set H of all those transformations in the set J which have *regular* frame matrices. We say that H is the set of *regular transformations* in J.

[14] Two transformations of the set J are "equal" when their schedules are exactly the same.

It is clear that H contains the identical transformation, defined by the schedule $Q=[(a_{ij}), a_i]$ in which $a_{ij}=1_n(i=j)$, $a_{ij}=0_n(i\neq j)$, $a_i=0_n$ (every index i). Here, as heretofore, we employ the designations 0_n and 1_n respectively for the zero and unit matrices of the range $R\{n\}$ in S.

By an argument based upon the *lemma*, a significant theorem may now be established:

Theorem 1: If T_a is any transformation in H, there exists, in H, an unique transformation T_b such that the schedule of the product T_aT_b is Q; and Q is likewise the schedule of the product T_bT_a.

This theorem asserts that (1) any *regular* transformation T in J has an unique inverse T^{-1}, and (2) T^{-1} is regular and has T for its inverse.

Proof: We suppose, first, that T_a is any *homogeneous* transformation in H (any transformation in H with the schedule $[(a_{ij}), a_i]$ in which $a_i=0_n$, the zero matrix of the range $R\{n\}$, for every index i). The frame matrix G_a of T_a is regular, and has an unique reciprocal[15] G_a^{-1} in the range $R\{g\}$. Hence that homogeneous transformation T_b of J which has the frame matrix G_a^{-1} is regular, and lies in H. By the *lemma*, T_b is manifestly an unique inverse to T_a in the set H.

Now let T_a be any transformation in H. Let $y_i=z_i+a_i$ $(i=1, 2, \cdots, f)$, these sums being formed, of course, in the range $R\{n\}$ of matrices. Substituting in the equations of T_a, we obtain the equations of a transformation T_c in H—a transformation converting the sequence $x_1, x_2, \cdots, x_f$ into the sequence $z_1, z_2, \cdots, z_f$. Since T_c is of homogeneous type, it has an unique inverse T_c^{-1}. Replacing z_i, in the equations of T_c^{-1}, by y_i-a_i, and simplifying (by operations in the range $R\{n\}$), we determine the equations of a transformation T_a^{-1} which is the unique inverse of T_a in H.

The argument is completed by the observation that if G_a, G_b denote any two matrices, of the range $R\{g\}$, such that $G_aG_b=1_g$, the unit matrix of the range, then also $G_bG_a=1_g$ (See 7, Section 5).

We have thus a procedure for the actual determination of the equations of the inverse transformation of which the existence is asserted, the required operations being performed *in the underlying scale S itself*. As will be indicated in examples below, it is frequently possible and convenient to find the inverse transformation by elimination processes carried out *in the range* $R\{n\}$, without descending to the scale S.

The set H obviously constitutes a *group* of transformations, this group being finite if the scale S is finite.

9. *Construction of Transformations of the Group H*

The following modifications of a matrix of any range in any scale will be called *elementary*:

(1) interchanging rows and columns; (2) adding, to every element of any row (column), α times the corresponding element of another row (column),

[15] See (9), Section 5.

where α denotes any scalar (element of the underlying scale S); (3) multiplying every element of any row (column) by a *regular* scalar, and every element of another row (column) by the reciprocal of that scalar; (4) interchanging two rows (columns); (5) changing the sign of every element of a row (column).

The value of the determinant of the matrix is, of course, not changed by (1), (2), or (3); and is changed only in sign by (4) or (5).

Now consider the special matrix ${}_{g}I_{\beta}$ of the range $R\{g\}$ in the scale S. This matrix is so defined that it differs from the unit matrix 1_g of the range only at the intersection of the last (g-th) row and last column, where it has the scalar β instead of the scalar 1. Successions of elementary modifications may evidently be applied to ${}_{g}I_{\beta}$ in such manner as to alter its appearance completely, while leaving the value, β, of its determinant unchanged. Selecting, as β, any *regular* element of the scale S, we have the means of constructing, quickly and easily, a variety of regular matrices of the range $R\{g\}$. We may, of course, use any one of these as the frame matrix of a transformation in the group H.

10. *Involutory Transformations of the Group H*

Let us call a transformation T, in J, *involutory* if T^2 (that is, TT) is the identical transformation, so that the schedule of T^2 is Q. When T is involutory, the determinant of the frame matrix of T^2 evidently has the value 1 in the scale S. Since the value of the determinant of a product of square matrices is obviously the product of the values of their determinants, we conclude that the value, δ, of the determinant of the matrix of T satisfies the equation $\delta^2=1$ in S. It follows that δ is a *regular*[16] element of S, and therefore that T is regular. Hence any involutory transformation in J is regular, and lies in the group H.

The following theorem is evident:

Theorem 2: If T_1 is an involutory transformation, and T any transformation, in H, then each of the transformations TT_1T^{-1} and $T^{-1}T_1T$ is involutory, and lies[17] in H.

For many cryptanalytic purposes, the following is an involutory transformation of sufficient complexity:

$$y_i = x_i - \lambda_i\tau\left(\sum_{j=1}^{f}\lambda_j x_j + \mu\right), \tag{2}$$

where $i=1, 2, 3, \cdots, f$; and $\lambda_1, \lambda_2, \cdots, \lambda_f, \mu$ is any sequence of $f+1$ matrices selected quite arbitrarily from the range $R\{n\}$ in the scale S; provided that

$$\sigma = \sum_{i=1}^{f}\lambda_i^2$$

is a *regular* matrix, and $\tau = 2\sigma^{-1}$, the symbol 2 denoting the element $1+1$ of the

[16] The equation $\delta^2=1$, in an arbitrary scale S, does not imply $\delta=\pm 1$. For example, in the scale $S(100)$, this equation has the four roots 1, 49, 51,99 (that is to say, ± 1 and ± 49).

[17] We have just noted that every involutory transformation in J lies in the group H.

scale S (so that τ is the sum of two matrices, each equal to the reciprocal of σ).[18]

Operations required for the application of formula (2) are to be performed in the range $R\{n\}$ of matrices in the scale S. We easily verify that the formula gives the equations of a transformation which is involutory. In fact, making two applications of this transformation, we obtain:

$$\begin{aligned} z_i &= y_i - \lambda_i\tau(\textstyle\sum\lambda_j y_j + \mu) \\ &= x_i - \lambda_i\tau(\textstyle\sum\lambda_j x_j + \mu) - \lambda_i\tau\{\textstyle\sum\lambda_j[x_j - \lambda_j\tau(\sum\lambda_q x_q + \mu)] + \mu\} \\ &= x_i - \lambda_i\tau\textstyle\sum\lambda_j x_j - \lambda_i\tau\mu - \lambda_i\tau\{\sum\lambda_j x_j - \sum\lambda_j^2\tau(\sum\lambda_q x_q + \mu) + \mu\} \\ &= x_i - \lambda_i\tau\textstyle\sum\lambda_j x_j - \lambda_i\tau\mu - \lambda_i\tau\sum\lambda_j x_j + \lambda_i\tau\sigma\tau\sum\lambda_q x_q + \lambda_i\tau\sigma\tau\mu - \lambda_i\tau\mu \\ &= x_i - 2\lambda_i\tau\textstyle\sum\lambda_j x_j - 2\lambda_i\tau\mu + 2\lambda_i\tau\sum\lambda_j x_j + 2\lambda_i\tau\mu = x_i. \end{aligned}$$

In other words, if we denote the transformation (2) by T, we have $T(x)=y$ and $T(y)=x$, so that $T^2(x)=x$.

The reductions made in the above verification of the involutory character of the transformation (2) will be easily understood if the reader bears in mind that $\tau\sigma=2_n$, where 2_n denotes the scalar matrix, in $R\{n\}$, of the scalar $2=1+1$ of S, and may be replaced by the scalar 2. It should also be recalled that in a mixed product of matrices and scalars we may, as explained in Section 5, shift the position of a scalar factor.

11. *Notations and Procedure in Examples*

Our illustrations will be based upon the scale $S(26)$. We shall give examples of ciphers based upon linear transformations in ranges of this scale. The extension of the method to other scales will be obvious, and will not require explicit treatment.

The following particular correspondence between $S(26)$ and the letters of the English alphabet will be adopted:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
m	*j*	*d*	*x*	*a*	*h*	*o*	*u*	*c*	*z*	*q*	*e*	*t*	*y*	*f*	*w*	*g*	*i*	*v*	*s*	*k*	*p*	*l*	*r*	*n*	*b*

or, in alphabetical arrangement:

a	*b*	*c*	*d*	*e*	*f*	*g*	*h*	*i*	*j*	*k*	*l*	*m*	*n*	*o*	*p*	*q*	*r*	*s*	*t*	*u*	*v*	*w*	*x*	*y*	*z*
4	25	8	2	11	14	16	5	17	1	20	22	0	24	6	21	10	23	19	12	7	18	15	3	13	9.

Any one of the 26! possible correspondences would serve equally well. But, to be explicit, we shall employ the foregoing.

The symbol ${}_nT_f$ will designate a transformation T which is performed in the range $R\{n\}$ of the scale $S(26)$, and is defined by f equations; such a transformation will convert a sequence of f matrices of $R\{n\}$ into another such sequence.

[18] Sections 13 and 14 present examples of the effective use of this formula.

Let it be desired to encipher a message by means of a transformation of the type ${}_nT_f$. Let the message be: $t_1, t_2, t_3, \cdots$, the t_i denoting simply the successive letters of the message as it is written out. Replacing the t_i by their corresponding elements of $S(26)$, we obtain the scalar sequence $q_1, q_2, q_3, q_4, \cdots$.

We now partition the q-sequence into subsequences of $k = n^2f$ elements each, writing $q_1q_2, \cdots, q_{k+1}\ q_{k+2}, \cdots, q_{2k+1}\ q_{2k+2}, \cdots$. If the last subsequence is incomplete, we fill it out, in any prearranged manner, to k elements.

Each subsequence is enciphered in the same way. The encipherment is accomplished by writing the subsequence, according to any convention, as a sequence of f square matrices, each of order n, in the scale $S(26)$, and subsequently transforming this sequence $x_1, x_2, \cdots, x_f$ of matrices, through a transformation of type ${}_nT_f$, into the sequence $y_1, y_2, \cdots, y_f$ of matrices. To decipher, we apply to the sequence $y_1, y_2, \cdots, y_f$ the transformation inverse to that used in encipherment.

The cipher subsequence actually transmitted is, of course, not the sequence $y_1, y_2, \cdots, y_f$ of matrices in $S(26)$, but the corresponding sequence of n^2f letters of the alphabet.

12. *Example 1*

The determinant of the matrix

$$\begin{pmatrix} 5 & 0 & 0 & 4 \\ 1 & 1 & 0 & 0 \\ 3 & 2 & 1 & 0 \\ 9 & 0 & 0 & 3 \end{pmatrix}$$

has the value[19] 5 in $S(26)$. Hence this matrix is regular; and the transformation

$$(1) \qquad y_1 = \begin{pmatrix} 5 & 0 \\ 1 & 1 \end{pmatrix} x_1 + \begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix} x_2 + \begin{pmatrix} 1 & 5 \\ 4 & 3 \end{pmatrix},$$

$$(2) \qquad y_2 = \begin{pmatrix} 3 & 2 \\ 9 & 0 \end{pmatrix} x_1 + \begin{pmatrix} 1 & 0 \\ 0 & 3 \end{pmatrix} x_2 + \begin{pmatrix} 2 & 0 \\ 1 & 6 \end{pmatrix},$$

of which it is the frame matrix, is regular. In this transformation, which we shall denote by T_1, the terms

$$\begin{pmatrix} 1 & 5 \\ 4 & 3 \end{pmatrix} \text{ and } \begin{pmatrix} 2 & 0 \\ 1 & 6 \end{pmatrix}$$

are, of course, chosen quite arbitrarily from the matrices of the range $R\{2\}$ in $S(26)$.

We readily find that the inverse transformation, T_1^{-1}, has these equations:

[19] See Section 9.

$$(3) \qquad x_1 = \begin{pmatrix} 11 & 0 \\ 15 & 1 \end{pmatrix} y_1 + \begin{pmatrix} 0 & -6 \\ 0 & 6 \end{pmatrix} y_2 + \begin{pmatrix} -5 & 7 \\ 1 & 16 \end{pmatrix},$$

$$(4) \qquad x_2 = \begin{pmatrix} 15 & -2 \\ -7 & 0 \end{pmatrix} y_1 + \begin{pmatrix} 1 & 6 \\ 0 & 1 \end{pmatrix} y_2 + \begin{pmatrix} 11 & -1 \\ 6 & 3 \end{pmatrix},$$

there being, throughout the work in $S(26)$, two alternative expressions for each element of the scale ($21 = -5$, $19 = -7$, etc.).

The equations (3) and (4) may be found by a simple elimination process in the range $R\{2\}$. The coefficient of x_2 in (2) is regular, and has the reciprocal[20]

$$\frac{1}{3}\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = 9\begin{pmatrix} 3 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 9 \end{pmatrix}.$$

Left-hand multiplication of each term of (2) by the product,

$$\begin{pmatrix} 0 & 4 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 9 \end{pmatrix} = \begin{pmatrix} 0 & 10 \\ 0 & 0 \end{pmatrix},$$

yields an equation which we subtract from (1), obtaining

$$(5) \qquad y_1 - \begin{pmatrix} 0 & 10 \\ 0 & 0 \end{pmatrix} y_2 = \begin{pmatrix} -7 & 0 \\ 1 & 1 \end{pmatrix} x_1 + \begin{pmatrix} -9 & -3 \\ 4 & 3 \end{pmatrix}.$$

The coefficient of x_1 in (5) being regular, we easily solve for x_1 in terms of y_1 and y_2. Then (4) is deduced in obvious manner.

In this example, $n = f = 2$. Given a message for encipherment, we first arrange it in subsequences of $n^2f = 8$ letters each, filling out the last subsequence, if necessary, by the adjunction of further letters according to the conventions of the cipher. Let the message be, for instance, SUSPEND ATTACK, so that the initial subsequence is SUSPENDA. Let it be agreed, as a cipher prearrangement, to write:

$$\begin{pmatrix} S & U \\ S & P \end{pmatrix}, \quad \begin{pmatrix} E & N \\ D & A \end{pmatrix},$$

thus determining the two matrices in $S(26)$,

$$x_1 = \begin{pmatrix} 19 & 7 \\ 19 & 21 \end{pmatrix}, \quad x_2 = \begin{pmatrix} 11 & 24 \\ 2 & 4 \end{pmatrix},$$

by means of the correspondence adopted in Section 11. Applying the transformation T_1 to the sequence x_1, x_2 of matrices, we obtain the sequence y_1, y_2:

$$y_1 = \begin{pmatrix} 17 & 9 \\ 12 & 2 \end{pmatrix} + \begin{pmatrix} 8 & 16 \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 5 \\ 4 & 3 \end{pmatrix} = \begin{pmatrix} 0 & 4 \\ 16 & 5 \end{pmatrix},$$

$$y_2 = \begin{pmatrix} 17 & 11 \\ 15 & 11 \end{pmatrix} + \begin{pmatrix} 11 & 24 \\ 6 & 12 \end{pmatrix} + \begin{pmatrix} 2 & 0 \\ 1 & 6 \end{pmatrix} = \begin{pmatrix} 4 & 9 \\ 22 & 3 \end{pmatrix}.$$

[20] See (9), Section 5.

Returning to the alphabet, we replace the sequence y_1, y_2 of matrices by

$$\begin{pmatrix} M & A \\ G & H \end{pmatrix}, \quad \begin{pmatrix} A & Z \\ L & X \end{pmatrix};$$

and the enciphered form of the initial message subsequence is $M\,A\,G\,H\,A\,Z\,L\,X$. In decipherment, we apply the transformation T_1^{-1} to the sequence y_1, y_2 of matrices, obtaining again the original matrix sequence x_1, x_2, and therewith also the original message subsequence *SUSPENDA*. The same procedure is followed with each message subsequence.

13. *Example 2*

If a cipher transformation can be made involutory without an appreciable weakening of the resistance offered to cryptanalysis, it is desirable, for many reasons, that this be done. Let us construct an involutory transformation of type ${}_2T_2$, employing formula (2), Section 10. Taking

$$\lambda_1 = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}, \quad \lambda_2 = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}, \text{ and } \mu = \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix},$$

we find that

$$\sigma = \lambda_1^2 + \lambda_2^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} + \begin{pmatrix} 9 & -1 \\ 5 & 14 \end{pmatrix} = \begin{pmatrix} 10 & -1 \\ 5 & 15 \end{pmatrix}$$

is regular. Thus we have:

$$\sigma^{-1} = \begin{pmatrix} 11 & -1 \\ 5 & 16 \end{pmatrix} \text{ and } \tau = 2\sigma^{-1} = \begin{pmatrix} 22 & -2 \\ 10 & 6 \end{pmatrix}.$$

It follows that:

$$-\lambda_1\tau = \lambda_1(-\tau) = \begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}\begin{pmatrix} 4 & 2 \\ 16 & 20 \end{pmatrix} = \begin{pmatrix} 4 & 2 \\ 14 & 8 \end{pmatrix}$$

$$-\lambda_2\tau = \lambda_2(-\tau) = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}\begin{pmatrix} 4 & 2 \\ 16 & 20 \end{pmatrix} = \begin{pmatrix} 10 & 0 \\ 0 & 10 \end{pmatrix}.$$

Therefore, by formula (2) of Section 10, the following transformation, which we shall call T_2, is involutory:

$$y_1 = x_1 + \begin{pmatrix} 4 & 2 \\ 14 & 8 \end{pmatrix}\left[\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}x_1 + \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}x_2 + \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}\right],$$

$$y_2 = x_2 + \begin{pmatrix} 10 & 0 \\ 0 & 10 \end{pmatrix}\left[\begin{pmatrix} 1 & 0 \\ 1 & -1 \end{pmatrix}x_1 + \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}x_2 + \begin{pmatrix} -1 & 2 \\ 0 & 1 \end{pmatrix}\right].$$

Its equations may be expressed:

$$(1)\qquad y_1 = \begin{pmatrix} 7 & -2 \\ -4 & -7 \end{pmatrix} x_1 + \begin{pmatrix} 10 & 0 \\ 10 & 16 \end{pmatrix} x_2 + \begin{pmatrix} -4 & 10 \\ 12 & 10 \end{pmatrix}$$

$$(2)\qquad y_2 = \begin{pmatrix} 10 & 0 \\ 10 & 16 \end{pmatrix} x_1 + \begin{pmatrix} -5 & -2 \\ 10 & 5 \end{pmatrix} x_2 + \begin{pmatrix} 16 & -6 \\ 0 & 10 \end{pmatrix}$$

the use of negatives being avoidable if only positive signs are desired.

The equations of T_2^{-1} are exactly the same as (1), (2) except that an interchange is made of x_1 and y_1, and of x_2 and y_2.

From T_2, we easily obtain, by Theorem 2, Section 10, further involutory transformations. Thus, denoting again by T_1 the transformation given in equations (1), (2) of Section 12, we know that each of the transformations $T_1^{-1}T_2T_1$ and $T_1T_2T_1^{-1}$ is involutory. These products may be determined from formulas (1) of Section 6, or by successive applications of the factor transformations. Following the latter method, we find that the product T_2T_1 is:

$$z_1 = \begin{pmatrix} 11 & 18 \\ 17 & 13 \end{pmatrix} x_1 + \begin{pmatrix} 10 & 2 \\ 10 & 6 \end{pmatrix} x_2 + \begin{pmatrix} 15 & 13 \\ 16 & 13 \end{pmatrix},$$

$$z_2 = \begin{pmatrix} 17 & 16 \\ 11 & 10 \end{pmatrix} x_1 + \begin{pmatrix} 21 & 8 \\ 10 & 3 \end{pmatrix} x_2 + \begin{pmatrix} 14 & 6 \\ 21 & 8 \end{pmatrix};$$

and that the (involutory) product $T_1^{-1}T_2T_1$ is:

$$(3)\qquad y_1 = \begin{pmatrix} 3 & 8 \\ 14 & 5 \end{pmatrix} x_1 + \begin{pmatrix} 24 & 4 \\ 12 & 2 \end{pmatrix} x_2 + \begin{pmatrix} 8 & 24 \\ 4 & 12 \end{pmatrix},$$

$$(4)\qquad y_2 = \begin{pmatrix} 6 & 8 \\ 12 & 14 \end{pmatrix} x_1 + \begin{pmatrix} 3 & 18 \\ 18 & 15 \end{pmatrix} x_2 + \begin{pmatrix} 6 & 14 \\ 0 & 24 \end{pmatrix}.$$

The cryptographic application of each of the two involutory transformations developed in this section is essentially the same as that of the non-involutory T_1 of the preceding section, and requires no separate discussion. The only difference—an important one, from the practical standpoint—is that the same transformation, with interchange of x_i and y_i, of course, is here employed for encipherment and decipherment.

14. *Example 3*

Let us determine an involutory transformation of type ${}_3T_2$. If we set:

$$\lambda_1 = \begin{pmatrix} 3 & 8 & 14 \\ 8 & 7 & 4 \\ 14 & 4 & 21 \end{pmatrix}, \quad \lambda_2 = \begin{pmatrix} 6 & 18 & 16 \\ 24 & 20 & 12 \\ 16 & 22 & 8 \end{pmatrix}, \quad \mu = \begin{pmatrix} 11 & 2 & 8 \\ 3 & 10 & 7 \\ 9 & 21 & 4 \end{pmatrix},$$

where

$$\sigma = \lambda_1^2 + \lambda_2^2 = \begin{pmatrix} 9 & 6 & 4 \\ 6 & 25 & 16 \\ 4 & 16 & 3 \end{pmatrix} + \begin{pmatrix} 22 & 14 & 24 \\ 10 & 4 & 18 \\ 24 & 20 & 12 \end{pmatrix} = \begin{pmatrix} 5 & 20 & 2 \\ 16 & 3 & 8 \\ 2 & 10 & 15 \end{pmatrix}$$

is regular, and μ is arbitrary, we find, by (9) of Section 5,

$$\sigma^{-1} = \frac{1}{21}\begin{pmatrix} 17 & 6 & 24 \\ 10 & 19 & 18 \\ 24 & 16 & 7 \end{pmatrix} = 5\begin{pmatrix} 17 & 6 & 24 \\ 10 & 19 & 18 \\ 24 & 16 & 7 \end{pmatrix} = \begin{pmatrix} 7 & 4 & 16 \\ 24 & 17 & 12 \\ 16 & 2 & 9 \end{pmatrix},$$

whence

$$\tau = 2\sigma^{-1} = \begin{pmatrix} 14 & 8 & 6 \\ 22 & 8 & 24 \\ 6 & 4 & 18 \end{pmatrix}, \quad \lambda_1\tau = \begin{pmatrix} 16 & 14 & 20 \\ 4 & 6 & 2 \\ 20 & 20 & 12 \end{pmatrix}, \quad \lambda_2\tau = \begin{pmatrix} 4 & 22 & 2 \\ 16 & 10 & 8 \\ 2 & 24 & 14 \end{pmatrix}.$$

By formula (2), Section 10, the transformation

$$y_1 = x_1 - \begin{pmatrix} 16 & 14 & 20 \\ 4 & 6 & 2 \\ 20 & 20 & 12 \end{pmatrix}(\lambda_1 x_1 + \lambda_2 x_2 + \mu),$$

$$y_2 = x_2 - \begin{pmatrix} 4 & 22 & 2 \\ 16 & 10 & 8 \\ 2 & 24 & 14 \end{pmatrix}(\lambda_1 x_1 + \lambda_2 x_2 + \mu)$$

is involutory. Its equations may be simplified to be

$$(1) \qquad y_1 = \begin{pmatrix} 3 & 6 & 2 \\ 16 & 23 & 8 \\ 2 & 16 & 13 \end{pmatrix}x_1 + \begin{pmatrix} 2 & 6 & 14 \\ 8 & 24 & 4 \\ 14 & 16 & 20 \end{pmatrix}x_2 + \begin{pmatrix} 18 & 6 & 6 \\ 24 & 20 & 22 \\ 2 & 2 & 16 \end{pmatrix}$$

$$(2) \qquad y_2 = \begin{pmatrix} 18 & 14 & 22 \\ 20 & 4 & 10 \\ 22 & 20 & 24 \end{pmatrix}x_1 + \begin{pmatrix} 15 & 16 & 20 \\ 4 & 13 & 2 \\ 20 & 8 & 11 \end{pmatrix}x_2 + \begin{pmatrix} 2 & 16 & 14 \\ 8 & 12 & 4 \\ 14 & 8 & 20 \end{pmatrix}.$$

Further involutory transformations of the type ${}_3T_2$ may, of course, be obtained from this by applying Theorem 2 of Section 10 and formulas (1) of Section 6; or by applying Theorem 2 of Section 10 and the procedure outlined at the close of Section 13.

In using the involutory transformation given by the equations (1) and (2) above, we first partition our message into subsequences of eighteen letters each, since $n^2f = 18$. We fill out the last subsequence, if it is incomplete, with any prearranged letters.

Consider, for instance, the message: *HOLD OUT. SUPPORTING AIR SQUADRONS EN ROUTE.* It contains two full subsequences. Let us treat the first of these: *HOLDOUTSUPPORTINGA*. We suppose that the convention adopted in the cipher is to write:

$$x_1 = \begin{pmatrix} H & 0 & L \\ D & 0 & U \\ T & S & U \end{pmatrix} = \begin{pmatrix} 5 & 6 & 22 \\ 2 & 6 & 7 \\ 12 & 19 & 7 \end{pmatrix}$$

$$x_2 = \begin{pmatrix} P & P & 0 \\ R & T & I \\ N & G & A \end{pmatrix} = \begin{pmatrix} 21 & 21 & 6 \\ 23 & 12 & 17 \\ 24 & 16 & 4 \end{pmatrix}$$

by means of the correspondence specified in Section 11. Substituting these matrices for x_1 and x_2 in the equations (1), (2) of the present section, we obtain:

$$y_1 = \begin{pmatrix} 25 & 14 & 18 \\ 14 & 22 & 23 \\ 16 & 17 & 13 \end{pmatrix} + \begin{pmatrix} 22 & 0 & 14 \\ 10 & 0 & 4 \\ 24 & 0 & 20 \end{pmatrix} + \begin{pmatrix} 18 & 6 & 6 \\ 24 & 20 & 22 \\ 2 & 2 & 16 \end{pmatrix} = \begin{pmatrix} 13 & 20 & 12 \\ 22 & 16 & 23 \\ 16 & 19 & 23 \end{pmatrix},$$

$$y_2 = \begin{pmatrix} 18 & 12 & 24 \\ 20 & 22 & 18 \\ 22 & 6 & 12 \end{pmatrix} + \begin{pmatrix} 19 & 21 & 0 \\ 15 & 12 & 19 \\ 10 & 16 & 14 \end{pmatrix} + \begin{pmatrix} 2 & 16 & 14 \\ 8 & 12 & 4 \\ 14 & 8 & 20 \end{pmatrix} = \begin{pmatrix} 13 & 23 & 12 \\ 17 & 20 & 15 \\ 20 & 4 & 20 \end{pmatrix}.$$

Hence the enciphered form of the subsequence is

$$\begin{pmatrix} Y & K & T \\ L & G & R \\ G & S & R \end{pmatrix}, \quad \begin{pmatrix} Y & R & T \\ I & K & W \\ K & A & K \end{pmatrix};$$

or, as it would be transmitted,[21] *Y K T L G R G S R Y R T I K W K A K.*

Substitution of the matrices y_1, y_2 in the same equations (1) and (2) above yields again the original matrices x_1, x_2, the equations having first been written, of course, with x_i and y_i interchanged ($i = 1, 2$).

Each message subsequence is enciphered and deciphered in the same manner.

15. *Concluding Notes*

All the transformations discussed in the foregoing pages are obviously applicable in any range $R\{n\}$ of any scale S, the special range $R\{1\}$ coinciding with S and yielding ordinary scalar transformations. Of interest in cryptography are not only the scales $S(n)$, and their various algebraic extensions, but also certain non-modular and infinite scales. In this connection, we note especially the scale S consisting of all positive and negative integers and zero in the field of rational numbers; any *regular* transformation in a range of this scale will have a frame matrix with determinant of value ± 1.

Plans have been completed for a novel type of computing machine capable of effecting the simultaneous and speedy evaluation of any desired number of

[21] When the entire message has been enciphered, it will normally be transmitted in the conventional five-letter groups: *YKTLG RGSRY* · · · ·

linear functions of any assigned sequences of elements in any scale of type $S(n)$, the linear functions having any arbitrarily selected scheme of coefficients. The machine, although originally designed for other purposes, may be used to apply very rapidly, without calculations of any sort, all transformations proposed in this paper for which the underlying scale is an $S(n)$, and even products of such transformations with widely variable ciphers of different type. From the point of view of cryptography, this circumstance lends exceptional interest to the scales $S(n)$.

Formula (2), Section 10, demands a sequence $\lambda_1, \lambda_2, \cdots, \lambda_f$ of f square matrices such that $\lambda_1^2+\lambda_2^2+\cdots+\lambda_f^2$ is a *regular* matrix. A great variety of sequences with this property can be determined very quickly, in any range of any scale, and for any positive integer f, by means of an interesting formula which will be the subject of special discussion elsewhere.

In any scale S, it is easy to set up an algebra for ranges of matrices whose elements are in turn matrices, the elements of these latter being again matrices, etc. But no important cryptographic advantages seem to arise from these further complications.

TWO FUNCTIONAL EQUATIONS WITH INTEGRAL ARGUMENTS

By PHILIP FRANKLIN, Massachusetts Institute of Technology

Professor E. T. Bell has recently indicated[1] that the general solution of the functional equations

$$f(x, n_1)f(x, n_2) = f(x, n_1 + n_2 + c), \tag{1}$$

$$f(x, n_1)f(x, n_2) = f(x, cn_1n_2), \tag{2}$$

in which the argument n is an integer $\geqq 0$, and the constant c is an integer $\geqq 0$, while x is a parameter, had a connection with the question of possible types of arithmetic; and asked what were the general solutions of these equations. We here obtain these general solutions, showing that the solution of the first involves a single function of x, while that of the second involves an enumerable number of such functions.

Theorem 1. *The general solution of* (1) *is* $[F(x)]^{n+c}$. We prove this by noting that, in consequence of (1), we have:

$$f(x, n-1)f(x, n+1) = f(x, 2n+c) = [f(x, n)]^2 \qquad (n = 1, 2, \ldots). \tag{3}$$

This shows that if $f(x, 0) = 0$, $f(x, n) = 0$ for all n; and also that if $f(x,0) \neq 0$, no $f(x, n)$ can vanish. In this latter case, we may rewrite (3) in the form:

$$\frac{f(x, n+1)}{f(x, n)} = \frac{f(x, n)}{f(x, n-1)} \cdots = \frac{f(x, 1)}{f(x, 0)} = F(x). \tag{4}$$

[1] This Monthly, vol. 37 (1930), p. 484.

This shows that

$$f(x, n) = f(x, 0)[F(x)]^n. \tag{5}$$

Finally, from (1),

$$[f(x, 0)]^2 = f(x, c) = f(x, 0)[F(x)]^c, \tag{6}$$

so that

$$f(x, 0) = [F(x)]^c, \tag{7}$$

and

$$f(x, n) = [F(x)]^{n+c}, \tag{8}$$

which is the general solution, since the excluded case reappears by putting $F(x) = 0$ in (8). This is the solution given by Professor Bell.

Theorem 2. *Let c be greater than 1, and let*

$$c = c_1^a c_2^b \cdots c_t^k, \quad a + b \cdots + k = s, \tag{9}$$

be the factorization of c into prime factors distinct from unity. Let the range of x be divided into two parts, denoted by x_0 and x_1. For the first part, take for all n:

$$f(x_0, n) = 0. \tag{10}$$

On the second part, take t functions $f(x_1, c_i)$ such that

$$f(x_1, c_i) \neq 0, \tag{11}$$

but otherwise arbitrary, and an enumerable number of functions

$$f(x_1, p), \tag{12}$$

one for each prime distinct from 1 and c_i, these being absolutely arbitrary. Then, if $f(x, 1)$ is any solution of

$$[f(x, c_1)]^a [f(x, c_2)]^b \cdots [f(x, c_t)]^k = [f(x, 1)]^{s+1}, \tag{13}$$

the values of $f(x_1, m)$, where m is any composite number with factorization:

$$m = p_1^\alpha p_2^\beta \cdots p_r^\kappa, \quad \alpha + \beta + \cdots + \kappa = q, \tag{14}$$

are given by:

$$f(x_1, m) = \frac{[f(x_1, p_1)]^\alpha [f(x_1, p_2)]^\beta \cdots [f(x_1, p_r)]^\kappa}{[f(x_1, 1)]^{q-1}}. \tag{15}$$

also, $f(x_1, 0) = 0$, unless all the $f(x_1, m) = 1$, when it may equal 1. This gives the general solution of (2) in terms of the functions of (11), (12) and the root in (13), together with the specification of x_0, and the values of x for which $f(x, 0) = 1$.

When $c = 1$, we separate the range as before, and retain (10). On the range x_1, we take

$$f(x_1, 1) = 1, \tag{16}$$

the functions (12) *arbitrary for all primes not unity, and use* (15) *to complete the solution.*

When $c=0$, *we must have:*

$$f(x_1, n) = 1, \tag{17}$$

which is to be combined with (10).

To prove the statements about the general case, we note that by a repeated application of (2), the right member of (13) is found to be

$$f(x, c^e), \tag{18}$$

and by using (2) and (9), the left member has the same value and the relation (13) is proved. This shows that if any $f(x, c_i)$ vanishes, the same is true of $f(x, 1)$ for that x, and since (2) gives:

$$[f(x, n)]^2 = f(x, cn^2) = f(x, 1)f(x, n^2), \tag{19}$$

we see that $f(x, n)$ vanishes for all n. Thus there is a range x_0 for which (10) holds, while in the complementary range x_1, (11) is satisfied, and

$$f(x_1, 1) \neq 0. \tag{20}$$

We next use (2) to obtain

$$f(x_1, m)[f(x_1, 1)]^{q-1} = f(x_1, c^{q-1}m), \tag{21}$$

and in view of (14), by (2) the numerator of (15) has the same value. Since (20) holds, we may divide out and establish (15). Thus all the relations on the functions $f(x, m)$ stated in the theorem are shown to be necessary consequences of (2).

To show that no further relations are imposed, we have merely to note that the value given by (15) is unchanged if unity is counted as a prime factor to any finite power, that it gives the correct value for m a prime, and with the convention just made for $m=1$, taking $1=1^a$ in place of (14). Thus (15) defines $f(x_1, n)$ for all n in terms of the fundamental functions. But, if n_1, n_2 and $c\,n_1\,n_2$ be decomposed into prime factors, and the corresponding functions in (2) are evaluated by (15), it is found that (2) becomes an identity in view of (9) and (13). Thus our method gives a solution, and it is the most general one possible since no unnecessary restrictions are imposed.

When $c=1$, we have in place of (2):

$$f(x, n_1)f(x, n_2) = f(x, n_1n_2), \quad c = 1. \tag{22}$$

This shows that

$$[f(x, 1)]^2 = f(x, 1). \tag{23}$$

If

$$f(x, 1) = 0, \qquad f(x, n) = f(x, 1)f(x, n) = 0, \tag{24}$$

and we are on the range x_0. If not, then (16) holds, and (15) is established as before, or deduced directly from (22).

When $c=0$, we have in place of (2):

$$f(x, n_1)f(x, n_2) = f(x, 0). \tag{25}$$

This gives, in particular,

$$[f(x, n)]^2 = f(x, 0), \tag{26}$$

which shows that if $f(x, 0)=0$, we are on the range x_0. Otherwise, the equation

$$[f(x, 0)]^2 = f(x, 0) \tag{27}$$

shows that

$$f(x_1, 0) = 1, \tag{28}$$

and

$$f(x, 0)f(x, n) = f(x, 0) \tag{29}$$

which follows from (25), establishes (17).

Equation (29), which holds for all values of c, shows that

$$f(x, 0) = 0, \tag{30}$$

unless $f(x, n)=1$ for all $n\neq 0$, when it may equal 1 by (27) which also holds for all values of c.

We note in conclusion that the whole difficulty of the present problem lies in the restriction on the range of n. If n were a continuous variable, the transformation $n=y-c$ in (1) and $n=y/c$ in (2) would reduce them to the cases $c=0$ and $c=1$ respectively, which have been extensively studied, and can be reduced to one another by a logarithmic transformation.[2]

---

[2] See Ex. 1, 2, in §38 of de la Vallée Poussin's *Cours d'Analyse*, vol. 1, Paris, 1921.

QUESTIONS AND DISCUSSIONS

EDITED by R. E. GILMAN, Brown University, Providence, Rhode Island.

The department of Questions and Discussions in the Monthly is open to all forms of activity in collegiate mathematics, including the teaching of mathematics, except for specific problems, especially new problems, which are reserved for the department of Problems and Solutions.

TWO MNEMONICS

By ALAN S. HAWKESWORTH, Washington, D. C.

The following mnemonic for π is due to Sir James Hopwood Jeans:

"How I want a drink, alcoholic of course, after the heavy chapters involving
3. 1 4 1 5 9 2 6 5 3 5 8 9
quantum mechanics."
7 9

Here is one which I have worked out for $\log_{10} \pi$:

"This Logarithm employs a zero character; mantissa follows in digits
0.4 9 7 1 4 9 8 7 2 6
precisely what I now give."
9 4 1 3 4

A REMARK ON QUADRANGULAR SETS

By ALBERT A. BENNETT, Brown University

It may be of interest to teachers of projective geometry to emphasize a few of the more fundamental relations of the subject by using to a greater extent than customary, a certain common concept here discusssed.

We shall consider a certain projective figure, $Q(ABC, DEF)$, composed of six elements, A, B, C, D, E, F, and subject to the following conditions:

I. The figure $Q(ABC, DEF)$ is completely determined if any five of its elements are given.

II. $$Q(ABC, DEF) = Q(BCA, EFD) = Q(CAB, FDE) = Q(CBA, FED) = Q(ACB, DFE) = Q(BAC, EDF) = Q(BDF, EAC) = Q(DFB, ACE) = Q(FBD, CEA) = Q(FDB, CAE) = Q(BFD, ECA) = Q(DBF, AEC).$$

1. *The transversal postulate.* The transversal postulate and its immediate corollaries state that if A, B, C, are the vertices of a non-degenerate triangle, and if D is a third distinct point of the line BC and E a third distinct point of the line CA, then there exists a unique point F as the intersection of the lines AB and DE. The six points constitute a figure, $Q(ABC, DEF)$, satisfying the two conditions stated.

2. *Desargues' theorem on perspective triangles.* If A', B', C', and A'', B'', C'' are corresponding vertices of two triangles perspective from a line, the triangles are perspective from a point. Let $A'B'$ meet $A''B''$ in F, let $B'C'$ meet $B''C''$ in D, and let $C'A'$ meet $C''A''$ in E, where by hypothesis D, E, F, are collinear

on the "axis of perspectivity." Let the lines $A'A''$, $B'B''$, meet in a point, P. The theorem states that $C'C''$ also passes through P. Let $A'A''$ meet the axis of perspectivity in A, let $B'B''$ meet it in B, and let $C'C''$ meet it in C. The theorem of Desargues is essentially equivalent to the statement that the quadrangular set of collinear points, A, B, C, D, E, F, denoted by $Q(ABC, DEF)$ is completely determined by any five of its points.

3. *Pascal's hexagon.* Given five points, A, B, C, D, E, in the plane with no three collinear, the theory of the Pascal hexagon is made the basis for a method of constructing other points of the conic determined as containing the given five points. In the theory of geometrical constructions, the most convenient form of the proposition is one freed of actual constructional details and may be stated as follows. If A, B, C, D, E be five distinct points of a non-degenerate conic, and if AD meets BE in P, then the line CP meets the conic in a determinate point F that may be constructed by the use of ruler alone. In this form, the six points, A, B, C, D, E, F, constitute a figure $Q(ABC, DEF)$ of the type mentioned, which is a quadrangular set of points on the conic.

4. *The inversive quadrilateral.* The theory of the construction of the sixth point of a quadrangular set in the complex plane (Argand-Wessel plane) is also a theory of intersections of certain circles in the inversive plane. Let A, B, C, D, E, be any given five distinct points of the inversive plane, which in the "general" case are such that no four are concyclic. We shall not stop to consider the various special cases. Draw circles, BCD, and AEC, which meet in C and in a second point, ordinarily distinct, that may be called P. The circles PAB and PDE, meet in a second point, F. This is the sixth point of the quadrangular set, $Q(ABC, DEF)$. In particular, this gives a construction for the product of complex numbers. As an example of a quadrangular set, one has[1] for any two numbers x, y, the following $Q(0, x, 1; \infty, y, xy)$. Hence we have the following construction, whose agreement with more traditional constructions is readily verified by elementary geometry. Draw a circle through the points 0, 1, and y. Draw the straight line through 1 and x. This is the circle through 1, x, and the infinite point. Let the line meet the circle again in the point, P. The circle through 0, x, and P, meets the line through y and P in the desired point xy. The fact that in this case $Q(ABC, DEF) = Q(AEC, DBF)$, for example $xy = yx$, leads to an interesting theorem on the concurrence of the four circles circumscribing the triangles of a quadrilateral.

5. *Skew lines in space.* Given five mutually skew lines, A, B, C, D, E. construct the two reguli determined respectively as meeting the three lines B, C, D, and the three lines A, C, E. Through each point P of the line C, there is a unique line m, which meets the three skew lines, B, C, D, and also a unique line n, which meets the three skew lines, A, C, E. The lines m, n, when distinct determine a plane, meeting the five given lines in five points of a quadrilateral, whose sixth point, Q, is projective with P. As P traces the line, C, Q traces in general a space

[1] Veblen and Young, Projective Geometry, vol. 1, p. 145

cubic which in special cases reduces to a line F in space. If the five lines lie in the linear congruence determined by any four of them, the discussion may be carried on as follows, by paraphrasing case 4 mentioned above, since the lines of a linear congruence may be represented by points on a non-degenerate quadric surface in three space, the geometry of which is identical with the geometry of inversion save for certain important questions of reality. Take the reguli, BCD and AEC, which meet in the line C and in a second line, ordinarily distinct, that may be called P. The reguli PAB and PDE, meet in a second line, F, which is the desired sixth element of the set.

RECENT PUBLICATIONS

EDITED by ROGER A. JOHNSON, Brooklyn College of the City of New York

All books for review should be sent directly to the editor of this department, at Brooklyn College, 66 Court Street, Brooklyn, N. Y., and not to any of the other editors or officers of the Association.

NEW BOOKS RECEIVED

Integralgleichungen. By Gerhard Kowalewski. Berlin, De Gruyter, 1930. 304 pages. 15 marks.

Geometrische Transformationen. By Karl Doehlemann. Second Edition, edited by Wilhelm Olbrich. Berlin, De Gruyter, 1930. 256 pages. 13 marks.

Non-Interpolating Logarithms, Cologarithms, and Antilogarithms. By Frederick W. Johnson. San Francisco, The Simplified Series Publishing Company, 1930. Price \$1.60, \$2.25, \$4.00, according to binding.

Topology. By Solomon Lefschetz. American Mathematical Society, Colloquium Publications, Volume XII. New York, 1930. x+410 pages.

Funktionentheorie. By Konrad Knopp. I. Grundlagen der allgemeine Theorie der analytischen Funktionen. Sammlung Göschen, 668. Berlin, De Gruyter, 1930. Fourth edition. 140 pages.

Geometry of Four Dimensions. By A. R. Forsyth. Cambridge, The University Press, 1930. Volume I, xxx+468 pages; Volume II, xii+520 pages. \$25.00 the set.

Accounting, Principles and Procedure. By Walter J. Goggin and James V. Toner. New York, Houghton Mifflin Company, 1930. viii+476 pages. \$3.50. Laboratory Manual, 272 pages. \$1.80.

The Quantum Theory. By Fritz Reiche. Translated by H. S. Hatfield and H. L. Brose. New York, E. P. Dutton, 1930. viii+280 pages. \$2.10.

Numerical Mathematical Analysis. By James B. Scarborough. Baltimore, The Johns Hopkins Press, 1930. xvi+416 pages.

Algebra for Junior and Senior High Schools. By J. W. Calhoun, E. V. White, and T. McN. Simpson. Richmond, Johnson Publishing Company, 1930.

REVIEWS

Contributions to the History of Determinants, 1900–1920. By Sir Thomas Muir, D.Sc., LL.D., F.R.S., C.M.G. Blackie and Son Ltd., London and Glasgow, 1930. pp. xxiii+408.

In this sequel to his classic four volume work on the history of determinants from 1693 to 1900, Sir Thomas Muir maintains the high level of thoroughness and interest which make the earlier volumes a delight. The plan of the present book is uniform with that of its predecessors, to which it is an indispensable adjunct. The publishers have spared no pains to make the easy, open pages attractive and intelligible at a glance, and they, with the author, are to be congratulated on a fine book.

Whether the reader is interested for its own sake in the theory of determinants, or whether he uses determinants as the merest incidents in his own work, he will find much in this volume to induce him at least to browse for a spell and enjoy the author's occasional pungent remarks on the miscellaneous fare offered. As Dr. Johnson observed of the incomparable haggis, "there is much fine, confused feeding" in a mathematical history, and in a historical account of determinants the tremendous feast resembles a Chinese banquet rather than a single, well cooked dish. To those who have acquired a more sophisticated palate, trained to the dry flavor of the greater modern algebraic theories, the theory of determinants as revealed by its history may seem rather lacking in coherence and more like an assortment of tidbits than a coordinated theory. The abstract part of it all, that which alone is entitled in a modern sense to the high designation "theory," can be stated in a couple of pages; the rest is mere repetition and variation, endlessly, on a theme which is neither intricate nor subtle.

In the twenty years covered in this volume the same duplication of results by one writer after another, as was noted frequently by the author in earlier volumes, is as conspicuous as ever. Seasoned mathematicians writing on determinants appear to be as negligent as the merest beginners in acquainting themselves with what their predecessors have done. There may be some merit in establishing known theorems all on one's own, but there is more in consigning the results to the wastebasket after discovering that they have already been printed three times or more. Some of the duplications reported in this volume seem almost incredible, and could hardly have been perpetrated honestly by anyone who had taken the trouble to consult Muir's earlier works. For this reason, if no other, the complete set of Muir's histories together with his eleven supplementary papers should be in every mathematical library. More important, anyone who itches to write anything on determinants in the classical notation might profitably spend half an hour running down the cause of his distress in Muir's histories; the odds are that he will be cured.

Another caution of a different kind is rubbed in repeatedly by a reading of Muir's historical studies: it is not the recurrent which is of greater interest, but the generating function or difference equation that gave rise to the recurrent. A determinant for the nth Bernoulli number, for example, may be, and probably

is, as futile as it is pretty. Only a second and more misguided Wronski imagines he has solved the riddle of the universe when he evolves an utterly unmanageable determinant of the nth order to express the supreme law he thinks he has discovered. It makes no difference whether the determinant be symbolized in Greek or Latin characters, or in the more mysterious looking Hebrew which some specialists on determinants favor; if the determinant is of the nth order and not almost pathologically degenerate, it is no advance over the humble generating identity of which it is a pretentious disguise.

The sequence of chapters (with eleven omissions noted and treated elsewhere by the author) follows the plan of the earlier volumes so closely that there is no need to retail it here. The extremely interesting interpolated Chapter I (α), devoted to Hadamard's approximation-theorem from 1900 to 1917, raises a point of particular historical interest, as Muir insists that Lord Kelvin's name has a claim to be attached to the theorem. Among other judicial remarks, intended no doubt to adjust priority, those introducing Chapter VI (alternants), comparing the determinantal aspects of East Prussia and the State of New York, cannot fail to amuse American readers. One would think that determinants should be the last thing on earth to inspire chauvinism or envy, hatred and malice, but apparently it is not so. Let us hope that the enthusiastic investigators mentioned, neither of whom is longer writing for publication through the usual media, are not cutting one another on the Elysian fields.

Muir's longer writings are always lightened by a human touch, which may take the form of anything from a dry joke to a warm appreciation. Nor is the reader left in any doubt as to what is or is not "important." This, to the reviewer, seems to be a strategic error in writing a scientific history. What the professional user of such a history wants is the facts, and nothing but the facts, presented to him in the most concise form consistent with clarity, and without the historian's personal opinions on those facts, even in footnotes; it does not greatly matter what the "general reader" or the dilettante would prefer. If there is any reason for supposing historians of scientific subjects to be less fallible than historians in any other field, it is not evident, and the documents in the case of the older-fashioned literary type of history seem to show that the personal opinions and interpretations of historians serve no useful purpose, except to reveal to curious psychologists the prejudices of the historians.

The entire history inevitably suggests comparison with the only other one of recent times devoted exclusively to a branch of pure mathematics. This comparison may be irrelevant, but as another reviewer ("A. C. A." in *Nature*, November 29, 1930) invites it in the words "if there exists anywhere a more detailed and comprehensive history of any branch of theoretical knowledge, one would be interested to hear of it," the material for a comparison may be briefly indicated. In round numbers, Dickson takes 1600 pages to present, in minute detail, the history of the theory of numbers from Pythagoras (or before), 500 B.C., to 1923; Muir takes 2400 to tell less minutely the incomparably simpler and shorter story of determinants from Leibnitz, 1693 to 1920, or, allowing for

the difference in type, about the same space. In range and in detail there is no common measure for the two histories. Nor is there in style; Dickson's, for a serious student, has the complete efficiency of a battery of machine guns; Muir's is like the leisurely sprinkling of a shady lawn with a garden hose. Those who object to having a hail of facts shot at them without mercy may consider how far they would be likely to penetrate hostile territory, bristling with difficulties, if armed only with a garden hose or a watering pot.

As the author frequently points out, there has been but little diminution, if any, in the rate of production of writings on determinants in the twenty years covered by this volume. It may be suggested, however, that the counting of titles is not a reliable index when, as in this history, any incidental use of determinants in a paper whose main object often is far other than a contribution to determinants, is emphasized by isolation as the one fact of apparent interest. And, in passing, it appears to the reviewer that such a dislocation of secondary matter frequently gives an erroneous impression of a writer's motives in attempting to contribute to mathematical literature at all. In some instances it seems that no more relevant estimate of a paper by picking out the determinants it contains is possible than if the compiler were to emphasize, let us say, the incidential use of linear equations or algebraic division. Nor is the matter greatly helped when the historian supplements the record of secondary facts with his personal opinion on their importance or the lack of it.

One gets the impression on reading this book that the author is somewhat chagrined by the dearth of striking contributions to determinants in recent years. A possible explanation for this lack may be the simple fact—if it is one—that the theory of determinants, as a theory, has petered out. One most striking contribution to the theory does not seem to be mentioned by the author. The name of Ricci does not occur in the list of authors reported in this book or in the preceding volumes of the history. Possibly a perusal of Ricci's paper of 1899, in which the "Systems E" appear, seemingly for the first time, may suggest to future historians the year in which the *theory* of determinants expired and was buried under the rich loam of an infinitely wider and more fertile field. Those who claim that determinants are a comparatively trivial incident in the vaster and simpler theory of tensor algebra seem to have the right on their side.

A modern reading of one paper abstracted in the present volume might have suggested to the historian that the dearth of fundamental advances he deplores is due to the nature of the subject rather than to a lack of imagination on the part of the investigators. For, it seems to the reviewer, the entire significance of E. H. Moore's "Fundamental Remark Concerning Determinantal Notation, etc.," of 1900, has been completely missed by the historian. Between them, Ricci and Moore buried the theory of determinants in 1899–1900. Subsequent progress seems to show that this funeral is the fundamental development which the historian misses in his researches.

It may be too optimistic to hope that determinants will fade out of the mathematical picture in a generation; their notation alone is a thing of beauty

to those who can appreciate that sort of beauty. But it would seem to be well worth someone's trouble to write a short, accessible tract on determinants from a modern point of view, revealing their true simplicity and their strictly incidental character, as a historical pendent to Spottiswoode's paper of 1851 in which the now apparently obsolete theory was first didactically presented. The proof of the multiplication theorem by tensor algebra, for example, is a matter of two short lines, both obvious.

Whatever the future of determinants is to be, there can be no doubt that Sir Thomas Muir's history will have no serious rival in its own field. In bringing to a close this fascinating story of a subject which claimed a considerable share of the attention of the great algebraists of the nineteenth century, Sir Thomas Muir has made all who are interested in the scientific history of science his permanent debtors.

E. T. BELL

Number. By Tobias Dantzig. New York, The Macmillan Company, 1930. viii +260 pages. $3.50.

The superb Gothic towers of Quimper Cathedral are slightly marred by many stone curlicues extruding from the sides of the fine spires. While gazing with thorough enjoyment at the Cathedral, my first remark was the rather silly and unappreciative one, "I wish those spires had a shave." In undertaking this review, I rather fear that I may appear in a similar manner to emphasize slight blemishes at the expense of expressing the real appreciation that the structural soundness and vital interest of the book deserve.

There is no more comforting thought than that the human mind exploited as it often is by activities on the level of jazz and garrulous bridge can rise to the appreciation of mathematics and the other fine arts; and there is no more amazing story than that of the development, accurate analysis and successive generalizations of the concept of number. Professor Dantzig has undertaken the almost impossible task of telling this story to the mathematically untrained but highly intelligent layman, and has performed it remarkably well. To say that the trained mathematician will be even more interested in it than will the layman is not to disparage the readability of the work, but to praise its fundamental accuracy.

Chapter I, II and V, on *Fingerprints*, *The Empty Column*, and *Symbols*, deal largely with the conjectures concerning the early, and with knowledge of the later, history of the development of the number system as we know it when we leave high school. The third chapter on *Number Lore*, though occupying a somewhat isolated position in the book, gives insight into the origins of number theory, the rest of the book being motivated by the needs of analysis. The main body of the work is a description of the continued extension of the number system that has been necessitated by the enlarging demands of analysis. Even this description gives the impression of a somewhat artificial division that does

not exist in the book since much of the early chapters is devoted to the same theme as the later.

Mathematicians have successively demanded "closure," under the processes of counting, subtracting, dividing, successive approximation, and the solution of algebraic equations. Repeatedly with irrational, but not blind, faith they have played with the symbols for an enlarged but uncreated number system. Repeatedly, under the goad of conscience, they have constructed a system to go with these symbols. The process has been like the growth of a city. First the city becomes crowded, then the optimistic real estate man gives such names as "Fairview Boulevard" or "Sweet Briar Road" to some can-infested suburban wood lot, but in time the dwellers do come, the roads are created to take the names previously given, the city again becomes overcrowded and the process restarts. But this is not the whole story of the city; there must be some interested in improving the older portions. Nor is it possible, in mathematics, to anticipate all future criticisms; an ever present need compels the redefining of old concepts which, in light of new logical analysis, have become unsatisfactory, and thus we have the work of Cantor and Dedekind in the last century. This picture of enlargement of scope and intensifying of rigor Professor Dantzig has given admirably.

There are one or two places, however, in which Professor Dantzig's bias is enough different from the reviewer's to elicit a remonstrance, and there are a few places, not in the inner structure, but on the surface where I still feel that the book "needs a shave."

I can not feel that *Number* does justice to the point of view of Kronecker and Brouwer. I doubt if it is in the nature of things that mathematics will be as limited in its processes as its most rigorous critics may believe, but I likewise feel that their criticism indicates the direction in which investigation must be carried on if we are not to leave in the body mathematical many inconsistencies. The works of Peano, Frege, and Russell and the remarkable recent work of Hilbert have done perhaps as much as have the intuitionists to show that mathematics is faced with a vital problem. As a history of the progress of the mathematical frontier, *Number* shows real insight into the past difficulties and the magnitude of the past accomplishments. This is the main task of the work. In that small portion of the book which deals with the present frontier, there is something of a land agent attitude in belittling the seriousness of the task ahead in as far as that task is in the direction of increasing logical rigor.

Just an illustrative remark or two as to the desired shave! In light of the outstanding recent work in number theory by Professor Dickson, the remark "The triangular and more generally polygonal numbers are of no scientific interest" needs the razor. On page 165, the author gives a completely erroneous notion of what the phrase "well ordered" means, defining it as what is usually called "linearly ordered" plus the notion of the order being well defined. This also is a little furry. Again on pages 129 and 130, we find such remarks as "When after a thousand-year stupor, European thought shook off the effect of the sleep-

ing powders so skillfully administered by the Christian fathers, the problem of infinity was one of the first to be revived" and in speaking of the loose way in which the mathematicians dealt with infinite processes we have "yet another cause may be discerned. It should be remembered that the brilliant minds of that period were all raised on scholastic doctrine. To minds whose logic was fed on such speculations as sacrament and atonement, trinity and trans-substantiations, the validity of infinite processes was a matter of small concern." In comparison, one should read the first chapter of Whitehead's *Science and the Modern World*, for instance, "It needs but a sentence to point out how the habit of definite exact thought was implanted in the European mind by the long dominance of the scholastic logic and scholastic divinity. The habit remained after the philosophy had been repudiated, the priceless habit of looking for an exact point and of sticking to it when found."[1] In light of this far more just appraisal of that remarkable period, the Middle Ages, this crop of whiskers seems almost Bolshevistic.

I hope these minor criticisms do not too greatly detract from sensing the real appreciation the reviewer wishes to express. By all means get the book and read it. You will enjoy it. You will feel that a wonderful tale has been well told, and if once in a while you too turn barber—well, you will enjoy that also.

M. H. INGRAHAM

Gewöhnliche Differentialgleichungen. By G. Hoheisel. Sammlung Göschen, No. 920. 2nd edition, Berlin, de Gruyter & Co., 1930. 159 pp.

This small, ridiculously inexpensive book contains a surprising amount of material, excellently presented.

The first chapter, which deals with equations of the first order, explains the usual formal methods of integration, proves the existence theorem by the Picard method and discusses singular solutions and singular points. Chapter II deals with equations of higher order, particularly with linear equations. Chapter III considers boundary value problems.

J. F. RITT

A Course of Analysis, by E. G. Phillips. Cambridge University Press, 1930. viii+361 pages.

This text, written by a member of the faculty of the University College of North Wales, is based upon a course of lectures which he has given there for several years to the mathematical honours students. While all the topics treated in this book are to be found elsewhere, there appears to be no other textbook in English covering exactly the same ground. The main purpose of the book, as stated in the preface, is to give a logical connected account of the subject, starting with the definition of *number* and proceeding from that in a natural sequence of steps. The author keeps in mind throughout that the course is for

[1] A. N. Whitehead: *Science and the Modern World*, The Macmillan Co., New York, 1926, pp. 17–18.

many students preparatory to courses in applied mathematics and physics. The examples (many of them original) have been chosen mainly to illustrate the fundamental concepts, and the type of example whose solution depends on manipulative dexterity alone has been deliberately excluded by the author.

The scope of the book may best be estimated from the list of chapter titles: (1) Number; (2) Bounds and limits of sequences; (3) Limits and continuity; (4) Differential calculus; (5) Infinite series; (6) Inequalities; (7) Integral calculus; (8) Extensions and applications of the integral calculus; (9) Functions of more than one variable; (10) Implicit functions; (11) Double integrals; (12) Triple and surface integrals; (13) Power series. Comments on a few of these chapters may be appropriate.

In chapter 1 is given a brief account of the concept of *number*. The author feels that the theory of real numbers is the foundation upon which rests the whole structure of the subject of mathematical analysis. While avoiding the details of the philosophical questions involved, the author shows that the foundations of the subject of *number* lie further back than the mere assumption that the natural numbers are "known." He points out the distinction between the concept of cardinal number and that of ordinal number. In the treatment of irrational numbers, Russell's modification of Dedekind's method is used as the definition.

Throughout the book prominence is given to the concept of the differential of a function, a concept which is especially valuable in the case of functions of more than one variable. Hence, in chapter 4, the author makes a distinction between functions which are derivable (possess derivatives) and those which are differentiable (possess differentials), and in chapter 9 he makes a similar distinction between partial derivatives and differential coefficients. Likewise in chapter 7, the author points out the distinction between definite integration, which may be thought of as an analytic substitute for an area, and indefinite integration (for which he proposes the name "calculus of primitives"), which is the inverse of integration.

Topics whose treatment makes them worthy of especial mention are: the inequalities connected with the names of Hölder, Minkowski, and Jensen (chapter 6); Hermite's method of integrating rational functions (chapter 7); and area of a curved surface (chapter 12).

As the author says in the preface, "Modern analysis requires great precision of statement." While for the most part the author lives up to this ideal, the reviewer regrets that he must call attention to the following errors and defects in this book.

First there are numerous errors that indicate lack of careful editing. It is obvious that the quantity $\omega = |x-a| + |y-b| + |z-c|$, mentioned near the bottom of page 76 is *not* the length of the diagonal of the rectangular parallelopiped which has (a, b, c) and (x, y, z) for opposite vertices. In the last footnote on page 120, there is mentioned a possibility which can never occur so long as only series of positive terms are considered. In lines 17–20 of page 123, U_n means the

sum of the first n terms of a certain infinite series, but U_{n-v} does not mean the sum of the first $n-v$ terms of that series. Finally in the line following (2) on page 325, n is used in two different senses in the same equation.

A more serious error occurs in Weierstrass's theorem on page 32. The proof as given there is entirely fallacious, as may be seen by taking any sequence of points decreasing toward a sequential limiting point.

As has been stated above, the author in general distinguishes between concepts which are usually treated as identical but which are in reality different. It is unfortunate therefore that he does not emphasize the difference between the concept of the differential of the ***dependent*** variable and the concept of the differential of the ***independent*** variable. He perpetrates on page 87 the so-called "proof" that $dx=\Delta x$. All that this proof shows is that if $y=x$, then the differential of the dependent variable y is equal to Δx. Or what is the same thing, it shows that the differential of x when considered as a function of the independent variable x, is Δx. But it tells us nothing about the differential of the independent variable itself. That is an entirely different concept and requires a new definition.

Finally the author states so many theorems in a form which is false at worst and ambiguous at best, that the author seems at times to be aiming for "great carelessness of statement" rather than for "great precision of statement." An example of this carelessness is found at the bottom of page 188, where the author states: "If $f(x)$ be a continuous function and $a \leqq \xi \leqq b$, then

$$\int_a^b f(x)dx = (b-a)f(\xi).$$"

If we interpret this as most readers would, it means that the conclusion is true for *any* number ξ of the interval (a, b). But in that form the statement is false. What the author means is that "if $f(x)$ be a continuous function and (a, b) a given interval, then there exists a number ξ such that $a \leqq \xi \leqq b$ and

$$\int_a^b f(x)dx = (b-a)f(\xi).$$"

False statements similar to this one may be found also on page 103, lines 2–5; on page 104, lines 12–18; and on page 189, lines 9–10 and 14–16. A statement which might be called ambiguous occurs on page 179, in the last three lines, where the author gives another approximate form of the theorem stated above.

HARRY MERRILL GEHMAN

An Introduction to Mathematics. By Isaiah Miller. New York, F. S. Crofts and Co., 1930. xiii+297 pages.

In the preface the author states that in preparing this book he has kept in mind two types of students: first, those who will never take additional work in mathematics; and second, those who will continue the work in science or agri-

culture for advanced degrees and will doubtless desire to pursue additional courses in mathematics. He has therefore attempted to write a book basic in the fundamental principles of mathematics and at the same time has made practical applications wherever possible. Considerable attention is paid to fundamental principles and the applications are good, especially those relating to agriculture. The reviewer wishes to commend this feature of the text.

It is a book of 209 pages, not including the tables, with about the same emphasis upon algebra as is found in other books in the field of freshmen mathematics, a somewhat smaller amount of trigonometry, a chapter on statistics, one on annuities and insurance, and an introduction to some of the elementary notions of analytic geometry and calculus.

The author states that college freshmen need considerable drill on the fundamental processes of algebra before attempting a very extensive study of mathematics. This idea has been carried out by the author and hence we find the book to be elementary in character. It should be a satisfactory text to use, especially where students come to college with only one year of algebra and one year of geometry. The reviewer recommends it for students with this sort of preparation who desire to take a course in freshman mathematics.

In a book of this size, with a considerable review of high school algebra, quite a little space given to applications, and a treatment of the topics listed above, an author must of necessity omit certain phases of college algebra and trigonometry. The reviewer believes that the author is justified in his choice of subject matter according to his first purpose; namely, that of writing a book for those who will never take additional work in mathematics. It is not quite clear just how the second purpose is to be carried out, that of preparing students for analytic geometry and calculus. While there is no uniform agreement upon what topics should be stressed, it seems that a student would be considerably handicapped if he entered a course in analytic geometry, to be followed by calculus, with no previous study of such topics in algebra as equations in the quadratic form, simultaneous quadratic equations, infinite geometrical progressions, harmonic progressions, the binomial theorem for negative and fractional exponents, partial fractions, series, variation, indeterminate forms, theory of limits, determinants, and some of the elements of the theory of equations. Since applications are stressed, other topics that might be considered are the use of the base e, the slide rule, and logarithmic paper. Similar remarks are true of the sections involving trigonometry. The student in later courses in mathematics might feel the need for a knowledge of such topics as the solution of trigonometric equations, radian measure, the polar form of a complex number, DeMoivre's theorem, periodicity, and inverse trigonometric functions. From the point of view of the applications the graphs of the trigonometric functions might well be a part of the course. There will be instructors who feel that more problems in trigonometry might have been included. However, this is not a serious objection as supplementary problems can always be provided by the instructor when the need arises.

The book is printed on good paper, the type used is good, and the pages are very pleasing to the eye. The figures are well drawn. However, in the figure on page 55, the lines might better not be at an angle of 45° with the x-axis. No typographical errors of importance were noted. A good set of tables is included, occupying about 80 pages, which will be sufficient for the needs of the students.

FREDRICK WOOD

PROBLEMS AND SOLUTIONS

EDITED by B. F. FINKEL, OTTO DUNKEL, AND H. L. OLSON

Send all communications about Problems and Solutions to B. F. Finkel, Springfield, Mo. All manuscripts should be typewritten, with double spacing and with margins at least one inch wide.

PROBLEMS FOR SOLUTION

Problems containing results believed to be new, or extensions of old results are especially sought. The editorial work would be greatly facilitated if, on sending in problems, proposers would also enclose any solutions or information that will assist the editors in checking the statements. In general, problems in well-known textbooks or results found in readily accessible sources, will not be proposed as problems for solution in the Monthly. In so far as possible, however, the editors will be glad to assist members of the Association in the solution of such problems.

3479. *Proposed by C. A. Rasmussen, University of Alabama.*

If B and C be two fixed points and A a variable point at which BC subtends a given angle and if E and F be the feet of the perpendiculars from B and C, respectively, to the opposite sides of the triangle ABC, determine the path of a point P, the intersection of FP with EP, if $\angle BEP$ and $\angle PEC$, respectively, remain equal to $\angle ECB$ and $\angle FBC$.

3480. *Proposed by G. W. Wishard, Norwood, Ohio.*

Prove the following theorem: *If 1 be annexed to any triangular number in the nonary scale of notation, the result will be another triangular number.* Thus, 1, 11 111, 1111, etc. *ad infinitum* are triangular numbers in the nonary system.

3481. *Proposed by J. A. Calderhead, Boston, Mass.*

Calculate the critical speed in a high speed shaft, and show that $l=6N^{-1}(3EIw^{-1})^{1/2}$ gives the safe length when $N=$critical speed in revolutions per minute, $w=$weight per unit length, $E=$modulus of elasticity, and $I=$moment of inertia.

3482. *Proposed by Nathan Altshiller-Court, University of Oklahoma.*

If the circumscribed and the inscribed spheres of a tetrahedron are concentric, the sum of the face angles of each trihedral angle of the tetrahedron is equal to two right angles.

3483. *Proposed by Mabel M. Young, Wellesley College.*

A is a fixed point, B a variable point on a circle with center at O. Show that the locus of the orthocenter of triangle AOB is a strophoid.

3484 *Proposed by S. A. Corey, Des Moines, Iowa.*

Obtain a two-parameter solution of the Diophantine equations,

$$r^2 + s^2 + t^2 = 2(v^2 + w^2) = x^2 + y^2 + z^2.$$

3485. *Proposed by J. M. Feld, New York, N. Y.*

Let the sides of triangle $A_1A_2A_3$ be trisected. A_{ij} is the trisection point on a_j nearer A_i. Let P_i be the intersection of $A_{ij}A_j$ and $A_{ik}A_k$ and let Q_i be the intersection $A_{kj}A_j$ and $A_{jk}A_k$. Prove:

(1) The triangles $P_1P_2P_3$ and $Q_1Q_2Q_3$ are homothetic to $A_1A_2A_3$ and the common homothetic center is the centroid of $A_1A_2A_3$.

(2) $$P_1P_2/A_1A_2 = \tfrac{1}{4},\ Q_1Q_2/A_1A_2 = \tfrac{1}{5}.$$

(3) If C is the intersection of $A_{23}A_3$ and $A_{12}A_2$, and D is the intersection of $A_{13}A_3$ and $A_{32}A_2$, CD is parallel to A_2A_3.

3486. *Proposed by E. C. Kennedy, College of Mines, El Paso, Texas.*

Find a function of x such that the integral of that function between the limits 0 and x is equal to the reciprocal of the original function.

UNSOLVED PROBLEMS

Solutions are requested for the remaining five unsolved problems proposed in 1914 which are reprinted below.

205 [1914, 55]. *Proposed by E. T. Bell.*

Show that in the usual arithmetical sense the form that follows admits of composition; give the requisite transformations, and indicate how several (if not all) solutions may be found. The variables are the x_i:

$$x_0^2 + nrx_1^2 + mrx_2^2 + mnx_3^2 + mnrx_4^2 + mn^2r^2x_5^2 + nr^2m^2x_6^2 + rm^2n^2x_7^2.$$

287 [1914, 55; 1919, 312]. *Proposed by Walter H. Drane.*

While sitting in an empaled enclosure, I noticed that the spokes of the wheels of passing automobiles, when viewed through the pickets of the fence, appeared to revolve more slowly than they really did, and in some instances even appeared to be revolving in a direction opposite to that in which they were really turning. Explain this optical illusion.

353 [1914, 55; 1919, 312]. *Proposed by Richard P. Lochner.*

The center of a sphere, radius $R = 5$ inches, is $a = 10$ inches above the surface of a sphere, radius $r = 12\frac{1}{2}$ inches. There is a point of light at $b = 1$ inch horizontally from a point $c = 10$ inches vertically above the surface of the first sphere. What is the area of the shadow which the upper sphere casts on the lower one?

291 [1914, 122]. *Proposed by Emma M. Gibson, Springfield, Missouri.*

The time of descent, down a rough inclined plane, of a spherical shell which contains a smooth solid sphere of the same material as itself is t_1. The time of

descent, down the same plane, of a solid sphere of the same material and radius as the shell is t_2. Determine the thickness of the shell.

From Loudon's *Elementary Theory of Rigid Dynamics*, p. 188.

299 [1914, 267]. *Proposed by B. F. Finkel, Drury College.*

A cone rests in two fluids which do not mix, with its vertex downwards and its base in the surface of the upper fluid; to find how much its density must be increased, that it may rest with its base in the common surface of the fluids.

From Walton's *Hydrostatical Problems.*

SOLUTIONS

3430 [1930, 261] *Proposed by Richard M. Sutton, California Institute of Technology.*

It is physically possible, given a large number of unit resistances, to make any resistance p/q between two points A and B, where p and q are integers. The result may be accomplished by connecting in parallel q groups of p resistances each, requiring (pq) resistances. However, it is usually possible to accomplish the same result by a fewer number of unit resistances. The problem is: "Find the minimum number of unit resistances necessary to make a resistance p/q between two points A and B in an electric circuit, p and q being both integers."

Solution by J. P. Dalton, University of Witwatersrand, Johannesburg, South Africa.

A neat problem! Its solution depends upon the self-evident facts that if x and y are integers (i) the minimum number of unit resistances required to assemble a *resistance* of x units is x *in series;* (ii) the minimum number of unit resistances required to assemble a conductance of y units, i.e., a resistance of $1/y$ units, is y *in parallel.* Consider now a resistance of p/q, where p and q are integers, prime to each other. Express p/q as a terminating continued fraction

$$\frac{p}{q} = r_1 + \frac{1}{c_1 +} \frac{1}{r_2 +} \frac{1}{c_2 +} \cdots .$$

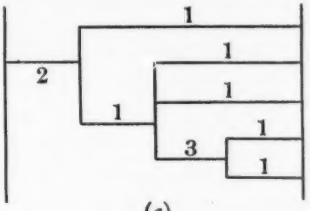
The partial quotients are resistances and conductances alternately, (hence the notation), and they determine the minimum network. The solution may be read thus:—A resistance r_1 in series with [a conductance c_1 in parallel with {a resistance r_2 in series with (a conductance c_2 in parallel with $\cdots$)}], bearing in mind that r_i signifies r_i unit resistances *in series*, while c_i signifies c_i unit resistances *in parallel.* The minimum number of unit resistances required is

$$\sum r_i + \sum c_i .$$

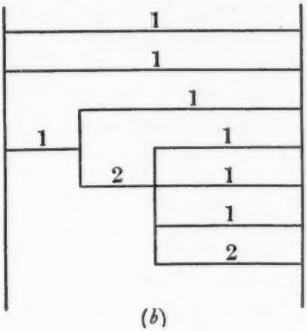
As a numerical example, resistances of 101/39 and 39/101 may be built from eleven units. For

$$(a)\ \frac{101}{39} = 2 + \frac{1}{1+} \frac{1}{1+} \frac{1}{2+} \frac{1}{3+} \frac{1}{2}; \text{ and } (b)\ \frac{39}{101} = 0 + \frac{1}{2+} \frac{1}{1+} \frac{1}{1+} \frac{1}{2+} \frac{1}{3+} \frac{1}{2}.$$

Hence the following networks:



(*a*)



(*b*)

A note by the Editors. If the denominator of the fraction p/q is a composite integer, where p and q have no common factor, then the partial quotients of the single continued fraction into which p/q is developed do not always give a minimum. This may be shown by examples. Thus

$$\frac{34}{15} = 2 + \frac{1}{3+}\,\frac{1}{1+}\,\frac{1}{3}, \qquad \text{9 units,}$$

whereas

$$\frac{34}{15} = 1 + \frac{1}{1+}\,\frac{1}{2} + \frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{2}, \qquad \text{8 units.}$$

Another example for which there are more than two decompositions is as follows:

$$\frac{31}{30} = 1 + \frac{1}{30} = \frac{1}{5} + \frac{1}{1+}\,\frac{1}{5} = \frac{1}{2} + \frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{7}$$

$$= \frac{1}{2} + \frac{1}{3} + \frac{1}{5} = \frac{1}{3} + \frac{1}{1+}\,\frac{1}{2+}\,\frac{1}{3}.$$

These decompositions require 31, 11, 11, 10, 9 units, respectively.

3436 [1930, 315]. *Proposed by Eugene M. Berry, Lynchburg College.*

Let p, q, and r be concurrent lines. Through any point on p draw lines

p', a, b, c, d, such that p' is perpendicular to p and that angles ab and cd are bisected by p. Show that the line aq-dr meets the line cr-bq on p' and meets the line cq-br on p.

I. *Solution by W. Randolph Church, Hightstown, New Jersey.*

Let the elements p, q, r, and p', a, b, c, d, be given so as to satisfy the conditions as stated in the problem. With the point pp' as center, draw a convenient circle. With respect to this circle, construct the poles of all the given lines. Let them be called by the corresponding capital letters. A, B, C, D, P, and P' will be at infinity, but their directions will be definitely known. Join the poles just constructed so as to form the polars of the points of intersection of the given lines. Draw also aq-dr, cq-br, cr-bq and locate the corresponding points AQ-DR, CQ-BR, CR-BQ. From the fact that the angle between two lines is equal to the angle which the line joining their poles subtends at the center of the circle, it is immediately apparent that angle PQ-QC equals angle PR-RD and angle PQ-QA equals angle PR-RB, for it is given that angle p-c equals angle p-d and angle p-a equals angle p-b. From elementary theorems concerning congruence and parallels we can conclude that the line joining CQ-BR and AQ-DR is parallel to RQ. Now P, Q, R are collinear. That is, CQ-BR, AQ-DR and P are collinear. Consequently their polars are concurrent; that is, cq-br, aq-dr, and p are concurrent. Similarly, the line joining AQ-DR and CR-BQ is perpendicular to RQ; that is, AQ-DR, CR-BQ and P' are collinear; or finally, aq-dr, cr-bq and p' are concurrent.

Remark: The same method enables us, if desired, to show that the remaining trios of the following set are concurrent:

$$aq - br,\ cq - dr,\ p';\quad aq - br,\ dq - cr,\ p';\quad aq - cr,\ bq - dr,\ p';$$
$$aq - cr,\ dq - br,\ p;\quad aq - dr,\ bq - cr,\ p';\quad aq - dr,\ cq - br,\ p;$$
$$ar - bq,\ cr - dq,\ p';\quad ar - bq,\ dr - cq,\ p';\quad ar - cq,\ br - dq,\ p';$$
$$ar - cq,\ dr - bq,\ p;\quad ar - dq,\ br - cq,\ p';\quad ar - dq,\ cr - bq,\ p.$$

It would be shown at the same time that the following five lines are concurrent:

$$aq - br,\ cq - dr,\ ar - bq,\ cr - dq,\ p'.$$

II. *Solution by Otto Dunkel, Washington University.*

The pencil of lines a, b, c, d, p, p', with the vertex V, is projective with the pencil b, a, d, c, p, p'. Hence the following two ranges of points are projective.

$$(1)\qquad \begin{matrix} ra, rb, rc, rd, rp, rp', \\ qb, qa, qd, qc, qp, qp'; \end{matrix}$$

and, since $rp \equiv qp \equiv W$, the lines joining the two points vertically above one another in (1) meet in a point U. The last pair of points shows that U lies on p'.

Also, if we select any square matrix from (1), the lines joining the diagonal points meet on a straight line. Since ra-qa, rb-qb meet in V, and ra-qp, rp-qb, in W, this line is p.

The following two ranges of points on r are projective,

$$(2) \qquad \begin{matrix} ra, rb, rc, rd, rp, rp', \\ rb, ra, rd, rc, rp, rp'; \end{matrix}$$

and we have two projective pencils by joining the points of the first row of (2) with qa, and those of the second with qb. The rays qa-rp, qb-rp coincide in q, and hence corresponding rays meet on a straight line. Since qa-ra, qb-rb meet in V, and qa-rp', qb-rp' meet on p', this line is p'. Hence the pairs of lines qa-rb, qb-ra; qa-rc, qb-rd; qa-rd, qb-rc meet on p'. In a similar manner using the vertices qc and qd we find that the pairs of lines

$$qc - ra, qd - rb; \quad qc - rb, qd - ra; \quad qc - rd, qd - rc$$

meet also on p'.

Also solved by D. C. Duncan, Paul Wernicke, and G. A. Yanosik.

3437 [1930, 315]. *Proposed by Nathan Altshiller-Court, University of Oklahoma.*

A variable circle passes through a fixed point and is tangent to a fixed circle. Prove that the diametric opposite of the fixed point on the variable circle describes a central conic of which the fixed point is a focus and the fixed circle is the auxiliary circle.

State and prove the converse of this proposition.

State the corresponding proposition for the parabola.

Solution by H. T. R. Aude, Colgate University.

Using rectangular coordinates take the center of the given circle at the origin and let a be its radius. Let A be the given point and place it at $(c, 0)$. On the variable circle of radius r which passes through A and is tangent to the given circle let $P(x, y)$ represent the diametric opposite to A. The center D of the variable circle has then the coordinates $\frac{1}{2}(x+c)$, $\frac{1}{2}y$ and with $AP=2r$ it follows that, for $c>a$, $OD=r\pm a$ according as the variable circle has external or internal contact with the given circle; if $c<a$ the variable circle is only tangent internally to the given circle and $OD=a-r$. The following two equations express the above statements for AP and OD in all cases (also for $c=a$).

$$(1) \qquad 4r^2 = (x - c)^2 + y^2,$$

$$(2) \qquad 4(r \pm a)^2 = (x + c)^2 + y^2.$$

It follows by subtraction that $2r = \pm(a^{-1}cx - a)$, and eliminating r^2 we obtain the equation,

$$(3) \qquad a^2y^2 + (a^2 - c^2)x^2 = a^2(a^2 - c^2),$$

which is recognized as the equation of hyperbola or ellipse with the usual meaning for c and a, with the given point as a focus and the given circle for auxiliary circle. In case $c=a$, equation (3) becomes $y^2=0$, a limiting case of both the ellipse and the hyperbola.

The converse proposition, that all circles constructed on the focal radii of a central conic as diameter are tangent to the auxiliary circle, follows at once from the above when it is recognized that the expressions for $2r$, namely $a-a^{-1}cx$ and $a^{-1}cx-a$, respectively, are the focal radii of ellipse and hyperbola from the focus (c, 0).

For the parabola, the corresponding propositions are: If a variable circle is drawn so that it passes through a fixed point and is tangent to a fixed line, then the diametric opposite of the fixed point on the variable circle describes a parabola which has the fixed point for focus and the fixed line as tangent at its vertex. And the converse, that all circles, upon the focal radii of a parabola as diameter have for envelope the line which is tangent to the parabola at its vertex.

Also solved by Rufus Crane, William Hoover, and G. A. Yanosik.

3438 [1930, 315]. *Proposed by the late F. P. Matz.*

Solve

$$\int_0^{dy/dx} \frac{\cos w\,dw}{16+9\sin^2 w} = \frac{1}{12}\tan^{-1}(x).$$

Solution by Ralph P. Agnew, Cornell University.

The integrand is periodic and gives the value 0 when integrated over any interval of length 2π. Hence dy/dx may be expected to be a real multiple-valued function of x for certain values of x. On carrying out the indicated integration, we find that the given equation is equivalent to

$$\tan^{-1}\left(\frac{3}{4}\sin\frac{dy}{dx}\right) = \tan^{-1}x, \tag{1}$$

where the left member lies between $-\pi/2$ and $\pi/2$, its algebraic sign agreeing with that of $\sin(dy/dx)$. Thus we see that if the given equation is to have a solution for dy/dx, its right member must represent the principal value of $\tan^{-1}x$. With this agreement, we find from (1) that $\sin(dy/dx)=4x/3$ and hence that

$$\frac{dy}{dx} = n\pi + (-1)^n \sin^{-1}\frac{4x}{3}, \quad |x| \leqq \frac{3}{4} \tag{2}$$

where n may be any integer, and the second term of the right member is $\geqq -\pi/2$ and $\leqq \pi/2$. From (2) we find

$$y = n\pi x + (-1)^n\left[x\sin^{-1}\frac{4x}{3} + \frac{1}{4}(9-16x^2)^{1/2}\right] + C, \quad |x| \leqq \frac{3}{4},$$

a result which holds when n is an integer, C is a constant, and the right member of the given equation is the principal value of the arctangent.

Also solved by S. F. Bibb, D. C. Duncan, E. C. Kennedy, and H. A. Meyer.

3440 [1930, 316]. *Proposed by A. Pelletier, Montreal, Canada.*

A triangle is circumscribed about a circle. Prove that the three following lines are concurrent: (1) the line joining the points of contact of any two sides; (2) the line joining the points of intersection of these sides with the bisectors of the opposite angles; (3) the line joining the feet of the altitudes on these sides.

I. *Solution by Mabel M. Young, Wellesley College.*

Let $A_1A_2A_3$ be the given triangle and I the centre of the inscribed circle. On any side, a_k, let G_k be the point of contact with the inscribed circle, H_k the foot of the altitude from A_k and I_k the point of intersection with the internal bisector of the opposite angle. We wish to prove that the lines H_kH_j, I_kI_j, G_kG_j are concurrent.

Let the escribed circle with centre, J_k, on the internal bisector of angle $A_jA_kA_i$ touch a_k in N_k. Through the points H_k, I_k, G_k, N_k draw lines perpendicular to a_k. These cut the internal bisector through A_k in A_k, I_k, I; J_k. Since these points form a harmonic set, the range $H_kI_kG_kN_k$ is harmonic and the rays joining these points to A_k form a harmonic pencil. But in any triangle, the altitudes meet in the orthocentre; the internal bisectors meet in the incentre; the lines from the vertices to the points of contact of the inscribed circle meet in the Gergonne point; and the lines from the vertices to the internal points of contact of the escribed circles meet in the Nagel point. Let these points be denoted, respectively, by H, I, G, N. Then H, I, G, N are projected from each vertex of the triangle by four harmonic rays and accordingly lie on a conic passing through A_1, A_2, A_3. Project A_i, H, I, G from A_k and A_j. Since the six points lie on a conic the two pencils are projective and the sections by a_k and a_j are perspective. Thus $A_iH_kI_kG_k \overline{\wedge} A_iH_jI_jG_j$ and lines joining corresponding points of these ranges are concurrent in a point P_{kj}. Since N_k and N_j are corresponding points on the perspective ranges, N_kN_j also passes through P_{kj}. In any triangle there are three such points of concurrence.

II. *Solution by George A. Yanosik, New York University.*

Let the given triangle ABC be the triangle of reference for the coordinates α, β, γ, which are so chosen that the center of the inscribed circle has the coordinates $(1, 1, 1)$. Then the equation of this circle is

$$\alpha^{1/2} \cos (A/2) + \beta^{1/2} \cos (B/2) + \gamma^{1/2} \cos (C/2) = 0.$$

The equation of a line (1) of the problem is that of the polar of C with respect to this circle, or

$$\mu \equiv \alpha \cos^2 (A/2) + \beta \cos^2 (B/2) - \gamma \cos^2 (C/2) = 0. \tag{1}$$

The internal bisector of angle A has the equation $\beta-\gamma=0$; the internal bisector of B has the equation $\alpha-\gamma=0$. Hence the equation of the corresponding line (2) is

$$\nu \equiv \alpha+\beta-\gamma=0. \tag{2}$$

The perpendicular from A to BC has the equation $\beta \cos B-\gamma \cos C=0$; the perpendicular from B to AC, the equation $\alpha \cos A-\gamma \cos C=0$. Hence the equation of the corresponding line (3) is

$$\alpha \cos A+\beta \cos B-\gamma \cos C=0 \text{ or } 2\mu-\nu=0. \tag{3}$$

Hence the three lines (1), (2), (3) meet in a point.

A note by the Editors. It is not necessary to use the equation of the inscribed circle, for the equation (1) may be obtained by a simple computation from the figure. If the equation of the inscribed circle is desired, it may be easily obtained from (1), since that line is the chord of contact of the two sides $\alpha=0$, $\beta=0$. The equation of the circle must then be of the form $\alpha\beta+k\mu^2=0$. Using the two sides $\beta=0$, $\gamma=0$ in the same manner, and then equating coefficients, the equation of the circle will be obtained. This appears to be a simpler method of derivation than that given in Salmon's *Conic Sections*.

Also solved by D. C. Duncan and William Hoover.

NOTES AND NEWS

Readers are invited to contribute to the general interest of this department by sending items to Professor H. W. Kuhn, Ohio State University, Columbus, Ohio.

Beginning with our January, 1931 issue the American Mathematical Monthly is to be included in the regular list of periodicals indexed in the "International Index to Periodicals" published by the H. W. Wilson Co.

Dr. Ganesh Prasad, Hardinge Professor of Higher Mathematics in Calcutta University and President of the Calcutta Mathematical Society, has given to that society an endowment for the purpose of awarding a prize and medal which is to be known as the Krishnakumari Ganesh Prasad Prize and Medal, in memory of his daughter. The award will be made every fifth year to the author of the best thesis embodying the result of original research in a topic connected with the history of Hindu mathematics before 1600 A.D. The subject of the thesis will be prescribed by the Council of the Calcutta Mathematical Society at least two years in advance.

At the Cleveland meeting of the American Association for the Advancement of Science, Assistant Professor C. F. Roos, of the department of mathematics of Cornell University, was elected permanent secretary, as successor to Professor B. E. Livingston, who becomes general secretary. Professor E. R. Hedrick was elected vice-president and chairman of Section A (Mathematics), and Professor G. C. Evans vice-president and chairman of Section K (Social and Economic Sciences).

At the Cleveland meeting of the American Association for the Advancement of Science an organization was formed for the purpose of promoting and improving the teaching of physics of college and university grade under the name of the American Association of Teachers of Physics. Regional as well as general meetings are to be held. The first general meeting will be at the Bureau of Standards in April in connection with the regular meeting of the American Physical Society. At that meeting Dr. A. W. Hull, assistant director of research of the General Electric Company, will present a paper on "The Training of Physicists for Industry."

Professor George Birkhoff, of Harvard University, has been elected Corresponding Member of the Royal Academy of Sciences of the Institute of Bologna.

Professor Wilhelm Blaschke, of the University of Hamburg, has recently delivered lectures, as visiting lecturer of the American Mathematical Society, at the following Universities and Colleges: Princeton, January 6, 7; Swarthmore, January 8; Columbia, January 14, 15; Cornell, January 22, 23; Chicago, January 27, 28; Iowa, February 4; Wisconsin, February 11; Ohio State, February 13, 14; Dartmouth, February 16, 17; Massachusetts Institute of Technology, February 19, 20, 24; Harvard, February 25; Brown, February 26. The subjects of these lectures were "Topological Questions of Differential Geometry," "Selected Topics from Differential Geometry," "Mathematical Problems of Nomography," and "The Geometrical Foundations of the Theory of Relativity." Professor Blaschke will lecture at The Johns Hopkins University as James Speyer Visiting Professor of Mathematics from March 2 to May 8, 1931, on "Topological Questions in Differential Geometry."

Professor Albert Einstein has been engaged in special research at the California Institute of Technology during the first semester of the present academic year.

Dr. R. A. Fisher, Chief Statistician of Rothamsted Agricultural Experimental Station, Harpenden, England will be in residence on the staff at the Iowa State College during the first half of the summer session, June 16 to July 24 and later will visit a number of colleges, universities and experiment stations throughout the country. In connection with Doctor Fisher's visit, Iowa State College announces a special group of summer courses covering the theory and application of statistics.

Professor Cassius J. Keyser lectured at Duke University, Durham, North Carolina, on March 12 and 13 on "Humanism and Pseudo-Humanism" and "The Human Significance of Science and Mathematics." Mr. Keyser is Professor Emeritus of Mathematical Philosophy at Columbia University.

Professor M. I. Pupin, of Columbia University, has received the decoration of the White Eagle of the First Order, conferred on him by Alexander I of Jugoslavia for outstanding services to the nation.

Professor G. B. Drummond, formerly at the Mississippi Agricultural and Mechanical College, has been appointed an assistant professor of mathematics at the Oklahoma Agricultural and Mechanical College.

Dr. Charles Hopkins has been promoted to be associate in mathematics at the University of Illinois.

Professor T. von Karman has been appointed professor of aeronautics at the California Institute of Technology.

Dr. Louis Lindsey, professor of applied mathematics at Syracuse University, has been granted leave of absence for the second semester of the present year. The time will be spent in travel and investigation in the South.

Associate Professor H. W. March, of the University of Wisconsin, has been promoted to a professorship of mathematics.

Miss Georgia E. Robinson has been appointed professor of mathematics at the Junior College, Centerville, Iowa.

Dr. J. A. Schouten, of the Delft Technical School, has been appointed professor of geometry at Princeton for the second semester of 1930–31.

Mr. C. E. Smith has been appointed assistant in the Chabot Observatory.

The following courses in mathematics are announced for the summer 1931:

Columbia University, July 6 to August 14. In addition to courses in trigonometry, solid geometry, analytic geometry, calculus, and methods of teaching secondary mathematics, the following advanced courses are offered: By Professor E. Kasner: Survey of mathematics; Geometric transformations. By Professor W. B. Fite: Groups of finite order. By Professor J. F. Ritt: Differential equations. By Professor P. A. Smith: Functions of a real variable.

Cornell University, July 6 to August 14. In addition to the usual elementary work, the following advanced courses will be offered. By Professor Virgil Snyder: Teachers' course. By Professor F. R. Sharpe: Elementary differential equations, and Advanced analytic geometry. By Professor W. A. Hurwitz: Theory of equations. By Professor D. C. Gillespie: Advanced calculus. By Professor W. B. Carver: Projective geometry. Reading and research work will be directed by Professors J. I. Hutchinson, Virgil Snyder, F. R. Sharpe, W. A. Hurwitz, W. B. Carver, D. C. Gillespie, C. F. Craig, B. W. Jones.

University of Illinois, June 22 to August 15. In addition to the usual courses in college algebra, trigonometry, analytic geometry, and calculus, the following advanced courses are offered: By Professor R. D. Carmichael: Functions of a complex variable; Linear differential equations. By Professor G. A. Miller: Theory of groups; History of mathematics. By Professor J. B. Shaw: Modern algebra. By Associate Professor Lytle: Fundamental concepts of mathematics; Teachers' course. By Assistant Professor Levy: Geometric transformations. By Dr. Hopkins: Theory of equations and determinants. By Dr. Ogg: Constructive and projective geometry.

University of Iowa. First term, June 8 to July 16. In addition to courses in college algebra, trigonometry, analytic geometry and calculus, the following subjects are offered. By Miss Ruth Lane: Subject matter and teaching of mathematics. By Professor Egon S. Pearson: Statistics; Seminar in statistics. By Professor Chittenden: Survey of mathematics; Modern theories of integration; Seminar in general topology. By Mr. Craig: Theory of equations. By Assistant

Professor Woods: Differential equations; Modern analytical geometry. By Dr. Earl: Mathematics of finance; Theory of approximation. By Assistant Professor Ward: Elementary mechanics; Ordinary differential equations (real variables). By Dr. Conkwright: Projective geometry; Theory of numbers. By the Staff: Reading and Research. Second Term, July 20 to August 20. By Professor Nordgaard: The History of mathematics. By Professor Reilly: Differential equations; Interpolation; Seminar in finite summation. By Professor Chittenden: Matrices and determinants; Introduction to general topology; Seminar in general topology. By Associate Professor Wylie: Meteors. By the Staff: Reading and Research.

Johns Hopkins University, June 29 to August 7. By Professor F. D. Murnaghan: College algebra; Differential and integral calculus; Functions of a complex variable *or* Calculus of variations (according to demand).

University of Kanas. First term, June 9 to July 18. In addition to the usual courses in college algebra, trigonometry, analytic geometry, and calculus, the following courses are offered: By Professor Ashton: Series; Seminar. By Professor Mitchell: Teachers course; Theory of numbers; Seminar. Second term, July 20 to August 14. By Professor Mitchell: Advanced algebra; History of mathematics; Seminar. By Professor Jordan: Advanced calculus.

University of Maine, July 6 to August 14. In addition to the usual elementary work, the following advanced courses are offered. By Associate Professor Bryan: Teachers' course. By Assistant Professor Lucas: Theory of equations; Analytic geometry in homogeneous coordinates. By Professor Willard: Theory of functions of a complex variable.

Massachusetts Institute of Technology. First period, June 16 to July 28: Courses in calculus and differential equations covering the prescribed work of the first two years. Second period, July 29 to September 9: Courses given in first period repeated. August 10 to September 12: Courses in algebra, solid geometry and trigonometry, in preparation for fall entrance examinations in those subjects. July 6 to July 31: Courses in methods of teaching mathematics in the Junior High School and the Senior High School. June 16 to July 7: Courses in advanced calculus and theoretical aeronautics. July 8 to July 28: Course in aeronautical continued. July 6 to August 3: Differential Equations, intended primarily for army officers.

University of Minnesota. First term, June 17 to July 25. In addition to the usual elementary work the following courses will be offered: By Professor Dunham Jackson: Vector analysis. By Professor Griffith C. Evans of the Rice Institute: Mathematical theory of economics. By Associate Professor Underhill: Theory of equations. By Assistant Professor Gladys Gibbens: Differential equations. By Professors Jackson, Underhill, and Gibbens: Reading in advanced mathematics. Second term, July 27 to August 29. By Professor Raymond W. Brink: Infinite series. By Dr. R. A. Fisher, Chief Statistician, Rothamsted Experimental Station, Harpenden, England: Statistical Methods. By Professor Griffith C. Evans of the Rice Institute: Potential theory. By

Professor Raymond W. Brink and Assistant Professor Elizabeth Carlson: Reading in advanced mathematics.

Stanford University, June 18 to August 29. In addition to the usual courses in calculus and differential equations, and a beginning course in the Theory of groups of permutations, the following courses will be given by Professor Edmund Landau (of the University of Gottingen): Foundations of arithmetic; Selected topics from the theory of functions.

Syracuse University. In addition to the usual courses in mathematics through the calculus, the following courses are offered: By Professor F. F. Decker: The teaching of algebra and geometry in secondary schools; and either the introduction to modern algebra or the theory of groups. By Professor A. D. Campbell: Analytic projective geometry or the general theory of the functions of a complex variable

University of Vermont. The following courses are offered by Professors Bullard, Butterfield, Millington and Swift: Courses in algebra, plane geometry for teachers, plane trigonometry, solid geometry, differential and integral calculus, differential equations, astronomy and history of mathematics.

Professor W. H. Bristol, inventor, and formerly professor of mathematics at Stevens Institute of Technology, has died at the age of seventy.

Dean Howard L. Hodgkins, for forty-eight years a member of the faculty of the George Washington University, died on Friday, February 13, 1931.

Mr. E. W. Hyde, for twenty-five years professor of mathematics at the University of Cincinnati, and formerly treasurer and actuary of the Columbia Life Insurance Company, has died at the age of eighty-seven.

CORRIGENDA

The following corrections should be made in the February issue of this MONTHLY:

On page 110 the signature at the end of the review of the Graham-John "Advanced Algebra" should be H. M. Hosford.

On page 69, the first line should read:

$$d = -2\alpha(y_2 - y_1)(x_2 - x_1)^{-1} + \tfrac{1}{2}(x_1 + x_2).$$

The error was the omission of the $+$ sign before the number $\frac{1}{2}$.

On page 71, the first displayed equation should read:

$$\{y_1(x_2 - x_1)^2[4y_1^2 + (x_2 - x_1)^2]^{-1}\} = \tfrac{1}{4}(x_2 - x_1)^2(y_1 + y_2)^{-1}.$$

The error was the omission of the -1 exponent which appears with the expression in brackets.

On page 78, in the 17th line the last term of the left hand member of the equation should be $81y_1^4$ instead of $81y_1^2$.

On page 80, in the first line the exponent $3/2$ should be $-3/2$; and in the denominator of the fraction in the next line the exponent $-3/2$ should be $3/2$.

Just Published

Plane Trigonometry

By WILLIAM WILDER BURTON
Clemson College, S.C.

This text has been designed for use in Liberal Arts colleges, universities, and engineering schools. It is the outgrowth of the author's experience in teaching the subject over a period of years and has departed somewhat from the modern tendency of concise treatment. The work has been presented in such a way that the student should be able to learn to rely upon himself to a considerable degree.

Published in three forms:
PLANE TRIGONOMETRY, WITH TABLES, $2.50
WITHOUT TABLES, $1.50
TABLES WITHOUT TEXT, $1.25

THOS. Y. CROWELL CO. 393 Fourth Ave., New York

A NEW MATH. TOOL

Edgar Dehn: ALGEBRAIC CHARTS

for solving quadratic, cubic and biquadratic equations. Price complete in special folder $1.00. Library edition $1.50 bound.

Patents pending

NOMOGRAPHIC PRESS 509 Fifth Avenue, New York

THE CHAUVENET PRIZE

In the year 1925, the MATHEMATICAL ASSOCIATION OF AMERICA established a prize of one hundred dollars for the best expository paper published in English during successive periods of five years by a member of the Association.

The purpose of the prize is to stimulate expository contributions in mathematical journals. The award does not apply to books, although the CARUS MONOGRAPHS are expository in character and on this score might be included. They carry their own reward in the form of a cash honorarium to each author.

The prize will be awarded hereafter every three years. The last award was in December, 1929, to Professor T. H. Hildebrandt. The next award will be in December, 1932, for the period of 1929-1931.

CONTENTS

The Information Bureau for Appointments 121

The Fifteenth Annual Meeting of the Association. By W. D. CAIRNS ... 121

Concerning Certain Linear Transformation Apparatus of Cryptography. By LESTER S. HILL 135

Two Functional Equations with Integral Arguments. By PHILIP FRANKLIN 154

QUESTIONS AND DISCUSSIONS: "Two Mnemonics" by ALAN S. HAWKESWORTH; "A Remark on Quadrangular Sets" by ALBERT A. BENNETT 158

RECENT PUBLICATIONS: New Books Received. Reviews by E. T. BELL, M. H. INGRAHAM, J. F. RITT, HARRY MERRILL GEHMAN, FREDRICK WOOD 160

PROBLEMS AND SOLUTIONS: Problems for Solution—3479–3486. Unsolved Problems. Solutions—3430, 3436, 3437, 3438, 3440 170

NOTES AND NEWS 178

DIRECTORY

EDITORIAL CORRESPONDENCE should be addressed to the EDITOR-IN-CHIEF, W. H. BUSSEY, 106 Folwell Hall, University of Minnesota, Minneapolis, Minn.

BOOKS FOR REVIEW should be addressed to R. A. JOHNSON, Brooklyn College, 66 Court Street, Brooklyn, N.Y.

BUSINESS CORRESPONDENCE should be addressed to the SECRETARY-TREASURER of the Association, W. D. CAIRNS, 33 Peters Hall, Oberlin, Ohio.

CHANGE OF ADDRESS: Members should send notice of any change of address to the SECRETARY-TREASURER, W. D. CAIRNS, Oberlin, Ohio, before the 10th of each month.

MEETINGS OF THE ASSOCIATION AND ITS SECTIONS

Fifteenth Summer Meeting of the Association, Minneapolis, Minnesota, Sept. 7-8, 1931.

The following is a list of the sections of the Association, with dates of those section meetings which have been scheduled for 1931.

ILLINOIS, Peoria, May 1-2.
INDIANA, Muncie, May 1-2.
IOWA, Davenport, May 1-2.
KANSAS, Topeka, Jan. 24.
KENTUCKY, April 15.
LOUISIANA-MISSISSIPPI, Natchitoches, La., March 13-14.
MARYLAND-DISTRICT OF COLUMBIA-VIRGINIA, Richmond, Va., May 9.
MICHIGAN, Ann Arbor, March 21.
MINNESOTA, St. John's University, Collegeville, May 16.
MISSOURI, St. Louis, November.
NEBRASKA, Lincoln, May.
OHIO, Columbus, April 2.
PHILADELPHIA, Philadelphia, Nov. 28.
ROCKY MOUNTAIN, Boulder, Colo., April 17-18.
SOUTHERN CALIFORNIA, Occidental College, Los Angeles, March 14.
TEXAS, Fort Worth, Tex., Jan. 31.

AFFILIATED ORGANIZATIONS: THE NEW ENGLAND ASSOCIATION OF TEACHERS OF MATHEMATICS. THE NATIONAL COUNCIL OF TEACHERS OF MATHEMATICS.

TWO THEOREMS ON THE PARTITIONS OF NUMBERS

By WALTER B. FORD, University of Michigan

Despite the very large existing literature upon the partitions of numbers the two following theorems do not appear to have been noted. In particular, they do not seem to occur in such extensive summary treatises as Dickson's History of the Theory of Numbers or MacMahon's Combinatory Analysis. At the same time they seem noteworthy inasmuch as they afford a means of determining rapidly the number of ways in which an integer n may be expressed as the sum of mth powers of other integers, either when repetitions among the latter integers are allowed or not allowed:

Theorem 1. *Let $P_{(n)}^{(m)}$ represent the number of ways in which the integer n may be expressed as the sum of m th powers of integers when repetitions among the latter integers are allowed. Then, if $\sigma_{(n)}^{(m)}$ represents the sum of those divisors of n which are m th powers of integers (including 1 and n itself if it is the m th power of an integer), the following recurrence relation exists:*

$$P_{(n)}^{(m)} = \frac{1}{n}\left[\sigma_{(1)}^{(m)} P_{(n-1)}^{(m)} + \sigma_{(2)}^{(m)} P_{(n-2)}^{(m)} + \cdots + \sigma_{(n-1)}^{(m)} P_{(1)}^{(m)} + \sigma_{(n)}^{(m)}\right].$$

Theorem 2. *Let $p_{(n)}^{(m)}$ represent the number of ways in which the integer n may be expressed as the sum of the m th powers of other integers when repetitions among the latter integers are not allowed. Then, if $\tau_{(n)}^{(m)}$ represents the sum of those divisors of n which are m th powers of integers (including 1 and n itself if it is the m th power of an integer) and which give odd quotients, minus the sum of the similar divisors which give even quotients, the following recurrence relation exists:*

$$p_{(n)}^{(m)} = \frac{1}{n}\left[\tau_{(1)}^{(m)} p_{(n-1)}^{(m)} - \tau_{(2)}^{(m)} p_{(n-2)}^{(m)} + \cdots + (-1)^{n-2} \tau_{(n-1)}^{(m)} p_{(1)}^{(m)} + (-1)^{n-1} \tau_{(n)}^{(m)}\right].$$

As to the proofs, let us consider first the simplest case of Theorem 1, namely, that in which $m = 1$. The actual (though inaccessible) value of $P_{(n)}^{(1)}$ will then be, as is well-known,[1] the coefficient a_n in the Maclaurin development

$$F(x) = \prod_{i=1}^{\infty} \frac{1}{1 - x^i} = 1 + \sum_{n=1}^{\infty} a_n x^n. \tag{1}$$

Now

$$\log F(x) = -\sum_{i=1}^{\infty} \log (1 - x^i) = \sum_{i=1}^{\infty} \sum_{j=1}^{\infty} \frac{x^{ij}}{j}.$$

Upon collecting the coefficients of the various powers of x here entering on the right, this equation takes the form

[1] See for example the paper by A. J. Kempner on *Partitio Numerorum* in this Monthly, vol. 3 (1923), page 360.